USER'S MANUAL

AXIS Q7406 Video Encoder Blade

Notices

This manual is intended for administrators and users of the AXIS Q7406 Video Encoder Blade, and is applicable for firmware release 5.11 and later. It includes instructions for using and managing the encoder on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial, for developing shell scripts and applications. Later versions of this document will be posted to the Axis Website, as required. See also the product's online help, available via the Web-based interface.
AXIS Q7406 supports ONVIF v1.0. For more information about ONVIF go to www.onvif.org For more information about enabling ONVIF go to the developers page at www.axis.com

Liability

Every care has been taken in the preparation of this manual. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Axis Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Axis Communications AB shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Intellectual Property Rights

Axis AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at http://www.axis.com/patent.htm and one or more additional patents or pending patent applications in the US and other countries.

This product contains licensed third-party software. See the menu item "About" in the product's user interface for more information.

This product contains source code copyright Apple Computer, Inc., under the terms of Apple Public Source License 2.0 (see http://www.opensource.apple.com/apsl/).
The source code is available from:
http://developer.apple.com/darwin/projects/bonjour/

Equipment Modifications

This equipment must be installed and used in strict accordance with the instructions given in the user documentation. This equipment contains no user-serviceable components. Unauthorized equipment changes or modifications will invalidate all applicable regulatory certifications and approvals.

Trademark Acknowledgments

Apple, Boa, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Netscape Navigator, OS/2, Real, QuickTime, UNIX, Windows, WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Axis Communications AB is independent of Sun Microsystems Inc.
UPnP™ is a certification mark of the UPnP™ Implementers Corporation.

Support

Should you require any technical assistance, please contact your Axis reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:
- download user documentation and firmware updates
- find answers to resolved problems in the FAQ database. Search by product, category, or phrases
- report problems to Axis support by logging in to your private support area
- visit Axis Support at www.axis.com/techsup

AXIS Q7406 Video Encoder Blade User's Manual
Rev. 2.2
Copyright© Axis Communications AB, 2008 - 2010
March 2010 Part no. 38829

Table of contents

Product Description 4
Key features 4
Overview 4
LED indicators 5
Using the video encoder 6
Access from a browser 6
Setting the root password 7
Access from the internet 7
Setting the root password over a secure connection 7
Video Streams 10
How to stream H.264 10
Motion JPEG 11
Alternative methods of accessing the video stream 11
Video 12
Video Stream 12
Camera Settings 13
Overlay Image 14
Privacy mask 14
Live View Config 15
Pan Tilt Zoom 18
Installing PTZ devices 18
PTZ configuration 19
PTZ controls 21
Using PTZ on video inputs 2-6 (AXIS 291 1U Video Server Rack) 22
Applications 23
Event Configuration 24
Event Servers 24
Event Types 24
Camera tampering 26
Motion Detection 27
Port Status 28
System Options 29
Security 29
Date & Time 30
Network 31
Ports & Devices 35
LED Settings 36
Maintenance 36
Support 36
Advanced 37
About 37
Resetting to the Factory Default Settings 37
Unit connectors 38
Pin assignments 39
Troubleshooting 42
Checking the Firmware 42
Upgrading the Firmware 42
Technical Specifications 46
General performance considerations 47
Optimizing your system 47
Glossary 48
Index 50

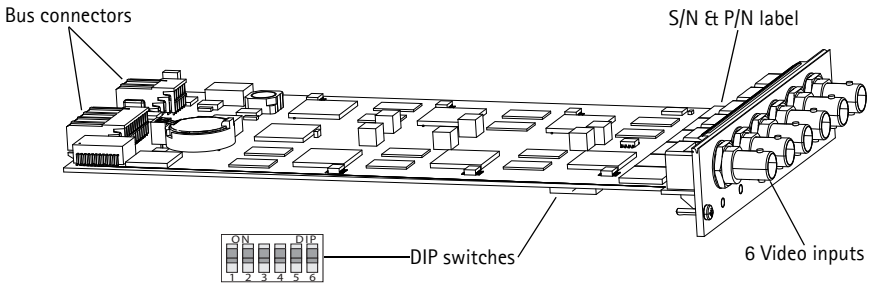
Product Description

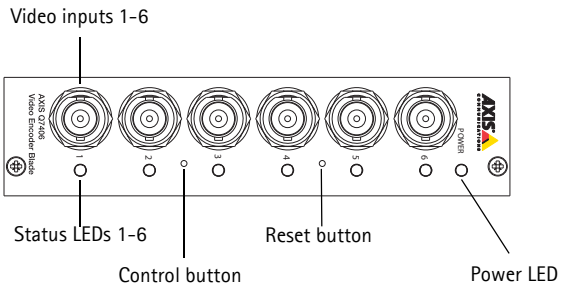
This manual applies to the AXIS Q7406 Video Encoder Blade.

Key features

- **High-density solution**
  When AXIS Q7406 blades, which have 6 video inputs, are used with AXIS Q7900 Rack, up to 84 analog cameras can be supported in one 4U, 19-inch rack.
- **Superb video quality**
  AXIS Q7406 offers the highly efficient H.264 video compression, which drastically reduces bandwidth and storage requirements without compromising image quality. Motion JPEG is also supported for increased flexibility.
- **Multiple H.264 streams**
  AXIS Q7406 can deliver multiple, individually configurable video streams from each channel at full frame rate in all resolutions up to D1 (720x480 in NTSC, 720x576 in PAL). This means that for each channel, several video streams can be configured with different compression formats, resolutions and frame rates for different needs.
- **Image setting adjustment**
  AXIS Q7406 also enables users to adjust image settings such as contrast, brightness and saturation to improve images before encoding takes place.
- **Intelligent video capabilities**
  AXIS Q7406 includes intelligent capabilities such as enhanced video motion detection and active tampering alarm. The encoder's external inputs and outputs can be connected to devices such as sensors and relays, enabling the system to react to alarms and activate lights or open/close doors.
- **ONVIF**
  This is a global interface standard that makes it easier for end users, integrators, consultants, and manufacturers to take advantage of the possibilities offered by network video technology. ONVIF enables interoperability between different vendor products, increased flexibility, reduced cost, and future-proof systems.

Overview





LED indicators

Status	Green	Steady green - normal operation
	Red	One flash - the corresponding channel is starting up
		Two flashes - the corresponding channel is resetting to factory default settings
		Steady red - hardware error on the corresponding channel
	Green/red	Flashes for no connection to AXIS Internet Dynamic DNS Service
Power	Green	Normal operation
	Green/Amber	Flashes for one or more channel upgrade

Using the video encoder

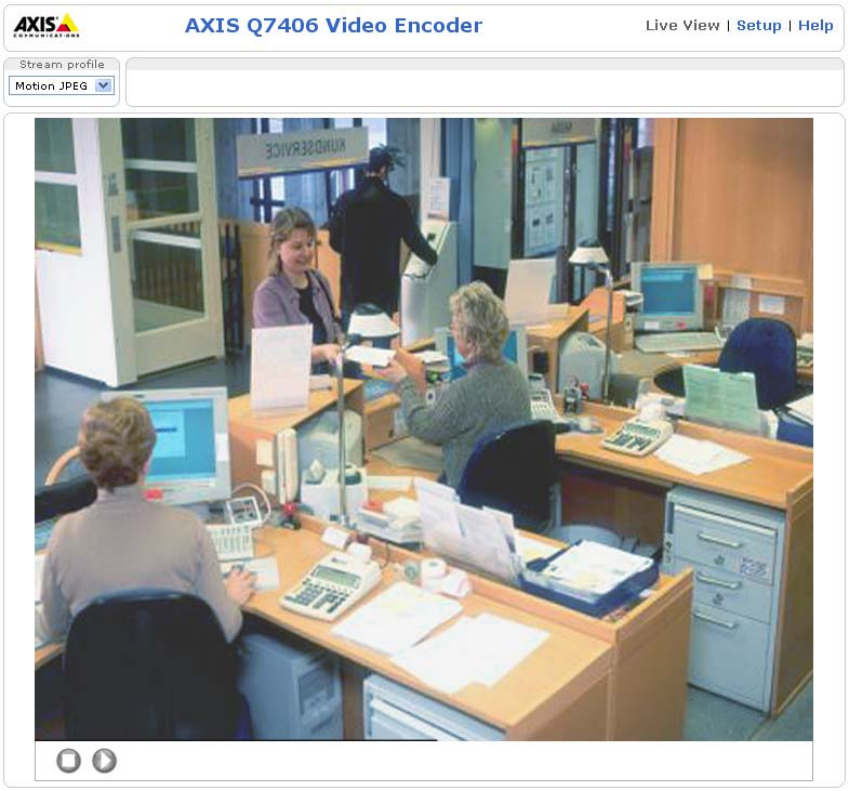
Refer to the installation guide supplied with your product in order to install the AXIS Q7406 Video Encoder Blade. The AXIS Q7406 can be used with most standard operating systems and browsers.

Notes:

- To view streaming video in Microsoft Internet Explorer, set your browser to allow ActiveX controls and install AXIS Media Control (AMC) on your workstation.
- QuickTime™ are also supported for viewing streaming H.264 video.
- If your workstation restricts the use of additional software components, the video encoder can be configured to use a Java applet for viewing Motion JPEG.
- The video encoder includes 6 decoder licenses for viewing H.264 video streams. This is automatically installed with AMC. The administrator can disable the installation of the H.264 decoder, to prevent installation of unlicensed copies.
- Each AXIS Q7406 has 6 serial numbers.

Access from a browser

1. Start a browser (Internet Explorer, Firefox).
2. Enter the IP address or host name of the one or more of the video inputs of the video encoder in the **Location/Address** field of your browser.
   To access the video encoder from a Macintosh computer (Mac OSX), click on the Bonjour tab and select one or more of the AXIS Q7406 video inputs from the drop-down list.
3. If this is the first time you are accessing the AXIS Q7406, see *Access from the internet*, on page 7. Otherwise enter your user name and password, set by the administrator.
4. The encoder's **Live View** page appears in your browser.

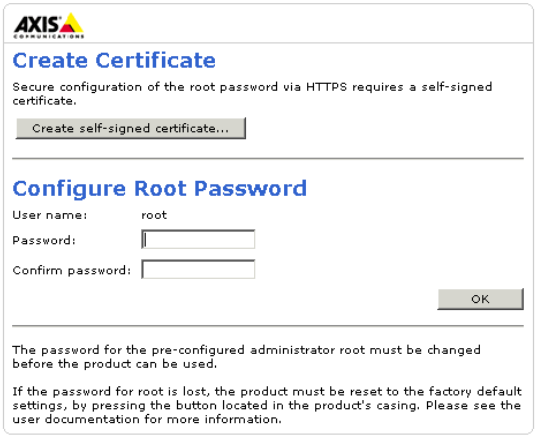


Note:

The layout of the **Live View** page may have been customized to specific requirements. Consequently, some of the examples and functions featured here may differ from those displayed on your own **Live View** page.

Setting the root password

1. When accessing the camera for the first time, the 'Configure Root Password' dialog appears.
2. Enter a password and re-enter to confirm. Click **OK**.
3. The **'Connect to...'** dialog appears. Enter the User name: **root**
4. Enter the password set in step 2, and click **OK**. If the password is lost, the camera must be reset to the factory default settings. See *Resetting to the Factory Default Settings*, on page 37.


AXIS
Create Certificate
Secure configuration of the root password via HTTPS requires a self-signed certificate.
Create self-signed certificate...
Configure Root Password
User name:
root
Password:
Confirm password:
OK
The password for the pre-configured administrator root must be changed before the product can be used.
If the password for root is lost, the product must be reset to the factory default settings, by pressing the button located in the product's casing. Please see the user documentation for more information.

Notes:

- The default administrator user name **'root'** is permanent and cannot be deleted.
- While setting the root password, click Yes to install the AXIS Media Control (AMC), if you are prompted to. You will need administrator rights on the computer to do this.

Access from the internet

Once connected, the camera is accessible on your local network (LAN). To access the camera from the Internet you must configure your broadband router to allow incoming data traffic to the camera. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the camera. This is enabled from **Setup > System Options > Network > TCP/IP Advanced**.

For more information, please see *NAT traversal (port mapping) for IPv4*, on page 33. See also the AXIS Internet Dynamic DNS Service at www.axiscam.net For Technical notes on this and other topics, visit the Axis Support web at www.axis.com/techsup

Setting the root password over a secure connection

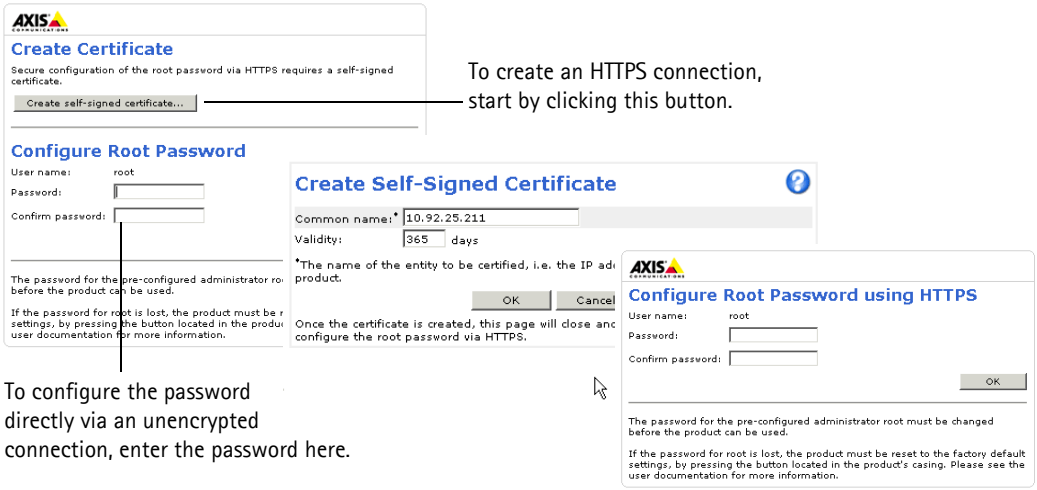
To gain access to the product, the password for the default administrator user root must be set. This is done in the **Configure Root Password** dialog, which is displayed when the video encoder is accessed for the first time.

To prevent network eavesdropping when setting the root password, this can be done via an encrypted HTTPS connection, which requires an HTTPS certificate (see note below).

To set the password via a standard HTTP connection, enter it directly in the first dialog shown below.

To set the password via an encrypted HTTPS connection, follow these steps:

1. Click the **Create self-signed certificate** button.
2. Provide the requested information and click **OK**. The certificate is created and the password can now be set securely. All traffic to and from the video encoder is encrypted from this point on.
3. Enter a password and then re-enter it to confirm the spelling. Click **OK**. The password has now been configured.


Create Certificate
Secure configuration of the root password via HTTPS requires a self-signed certificate.
Create self-signed certificate...
To create an HTTPS connection, start by clicking this button.
Configure Root Password
User name: root
Password:
Confirm password:
The password for the pre-configured administrator ro
before the product can be used.
If the password for root is lost, the product must be r
settings, by pressing the button located in the produ
user documentation for more information.
To configure the password directly via an unencrypted connection, enter the password here.
Create Self-Signed Certificate
Common name: 10.92.25.211
Validity: 365 days
*The name of the entity to be certified, i.e. the IP ad
product.
OK
Cancel
Once the certificate is created, this page will close anc
configure the root password via HTTPS.
Configure Root Password using HTTPS
User name: root
Password:
Confirm password:
OK
The password for the pre-configured administrator root must be changed before the product can be used.
If the password for root is lost, the product must be reset to the factory default settings, by pressing the button located in the product's casing. Please see the user documentation for more information.

Note:

HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt the traffic between web browsers and servers. The HTTPS certificate controls the encrypted exchange of information.

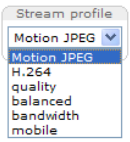
The default administrator user **root** cannot be deleted.

If the password for root is lost or forgotten, the video encoder must be reset to the factory default settings. See *Resetting to the Factory Default Settings*, on page 37.

The Live View page

If your video encoder has been customized to meet specific requirements, not all buttons and other items described below will be displayed in the **Live View** page. Below, find an overview of each available button:

General controls



The Stream Profile drop-down list allows you to select a customized or pre-programmed stream profile on the **Live View** page. Stream profiles are configured under **Video > Stream Profiles**, see *Stream Profiles*, on page 13 for more information.

Pulse - click this button to activate the output for a defined period of time - e.g. switching a light on for 20 seconds.

Active/Inactive - click these buttons to manually start and stop a connected device - e.g. switch a light on/off.

The **Action buttons** can trigger an event directly from the **Live View** page. These are configured under **Setup > Live View Config > Layout**.

The **Snapshot** button saves a snapshot of the video image currently on display. Right-click on the video image to save it in JPEG format on your computer. This button is primarily intended for use when the AMC viewer toolbar is not available.

AXIS Media Control toolbar

The AMC viewer toolbar (AXIS Media Control) is available in Microsoft Internet Explorer only. See *AXIS Media Control toolbar*, on page 9 for more information. AMC displays the following buttons:

The **Play** button connects to the Axis product and starts playing a media stream.

The **Stop** button stops the stream being played and terminates all network traffic with the Axis product.

The **Snapshot** button takes a snapshot of the current image. The location where the image is saved can be specified using the AXIS Media Control (AMC).

Click the **View Full Screen** button and the video image will fill the entire screen area. No other windows will be visible. Press **Esc** (Escape) on the computer keyboard to cancel full screen view.

The **Record** button is used to record the current video stream. The location where the recording is saved can be specified using the AXIS Media Control toolbar.

Pan/Tilt/Zoom controls

When in Center Mode, click on any part of the image other than its exact center and the camera will move so that the point you clicked on becomes the new center of the image.

If you select Emulate Joystick Mode, the camera moves in the direction of the mouse pointer. If you click and hold down on the left mouse button, and then point your cursor at the lower left hand corner of the image, the camera continues to move left and down until you release the mouse button.

Video Streams

The video encoder provides several image and video stream formats. Your requirements and the properties of your network will determine the type you use.

The **Live View** page in the video encoder provides access to H.264 and Motion JPEG video streams, and to the list of available stream profiles. Other applications and clients can also access these video streams/images directly, without going via the **Live View** page.

How to stream H.264

This video compression standard makes good use of bandwidth, and can provide high quality video streams at less than 1 Mbit/s.

Deciding which combination of protocols and methods to use depends on your viewing requirements, and on the properties of your network. The available options in AMC are:

<table>
<tr><td>Unicast RTP</td><td>This unicast method (RTP over UDP) should be your first consideration for live unicast video, especially when it is important to always have an up-to-date video stream, even if some images are dropped.</td><td rowspan="3">Unicasting is used for video-on-demand broadcasting, so that there is no video traffic on the network until a client connects and requests the stream.

Note that there are a maximum of 20 simultaneous unicast connections.</td></tr>
<tr><td>RTP over RTSP</td><td>This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.</td></tr>
<tr><td>RTP over RTSP over HTTP</td><td>This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.</td></tr>
<tr><td>Multicast RTP</td><td colspan="2">This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some images are dropped.

Multicasting provides the most efficient usage of bandwidth when there are large numbers of clients viewing simultaneously. A multicast broadcast cannot however, pass a network router unless the router is configured to allow this. It is not possible to multicast over the Internet, for example.

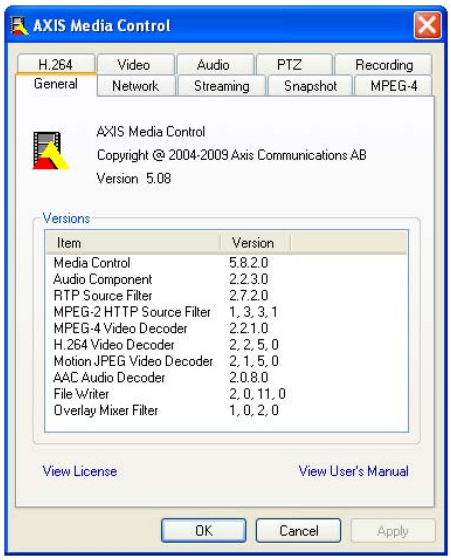
Note also that all multicast viewers count as one unicast viewer in the maximum total of 10 simultaneous connections.</td></tr>
</table>

AMC negotiates with the camera to determine the transport protocol to use in the order listed above. This order can be changed and the options disabled, to suit specific requirements.

Important!

H.264 is licensed technology. The video encoder includes one viewing client license. Installing additional unlicensed copies of the viewing client is prohibited. To purchase additional licenses, contact your Axis reseller.

AXIS Media Control (AMC)



The recommended method of accessing live video from the video encoder is to use the AXIS Media Control (AMC) in Microsoft Internet Explorer in Windows.

The AMC control panel can be used to configure various video settings. Please see the readme file included in the tool for more information.

The AMC control panel is automatically installed on first use, after which it can be configured.
Open the AMC Control Panel from:

- Windows Control Panel (from the Start menu)
- Alternatively, right-click the video image in Internet Explorer and click **Settings** to access the AMC window.

Motion JPEG

This format uses standard JPEG still images for the video stream. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion.

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream. The recommended method of accessing Motion JPEG live video from the video encoder is to use the AXIS Media Control (AMC) in Microsoft Internet Explorer in Windows.

Alternative methods of accessing the video stream

Video/images from the video encoder can also be accessed in the following ways:

- Motion JPEG server push (if supported by the client, Firefox, for example). This option maintains an open HTTP connection to the browser and sends data as and when required, for as long as required.
- Still JPEG images in a browser. Enter the path - http://<ip>/axis-cgi/jpg/image.cgi
- Windows Media Player. This requires AMC and the H.264 viewing client to be installed. The paths that can be used are listed below in the order of preference:
    - Unicast via RTP: axrtpu://<ip>/axis-media/media.amp
    - Unicast via RTSP: axrtsp://<ip>/axis-media/media.amp
    - Unicast via RTSP, tunneled via HTTP: axrtsphttp://<ip>/axis-media/media.amp
    - Multicast: axrtpm://<ip>/axis-media/media.amp

- To access the video stream from **QuickTime™** the following paths can be used:
    - rtsp://<ip>/axis-media/media.amp
    - rtsp://<ip>/axis-media/media.3gp

Notes:

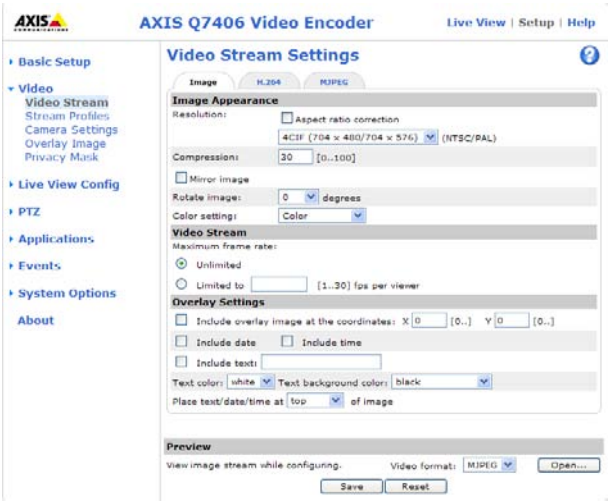
- The video encoder supports QuickTime 6.5.1 and later
- QuickTime adds latency to the video stream (up to 3 seconds)
- It may be possible to use other players to view the H.264 stream using the paths above, although Axis does not guarantee this
- <ip> = IP address

Video

This section describes how to configure the video encoder, and is intended for product **Administrators,** who have unrestricted access to all the configuration menus; and **Operators**, who have access to the settings for **Video & Image**, **Live View Config**, and **Event Configuration**.

You can configure the video encoder by clicking **Setup** in the top right-hand corner of the **Live View** page. Click on this page to access the online help that explains the configuration menus.

Video Stream



The video stream settings are separated in tabs:

- Image
- H.264
- MJPEG

Image

Image Appearance

Use these settings to modify the image resolution and compression. Setting the compression level affects the image quality and the amount of bandwidth required, the lower the compression, the higher the image quality with higher bandwidth requirements. The image can also be mirrored (reversed) and rotated. See the online help files for more information.

Video Stream

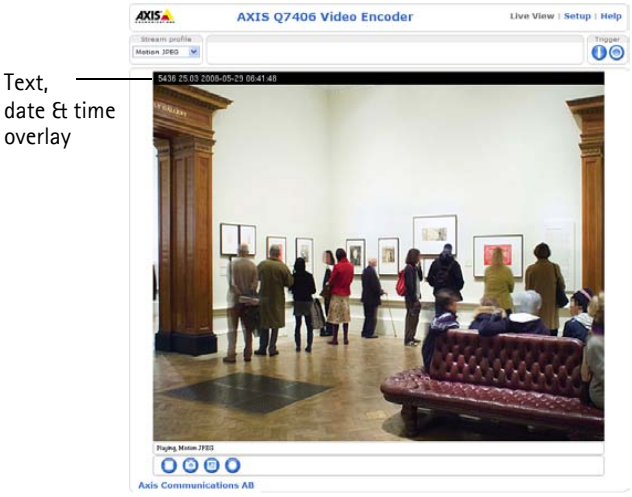
To avoid bandwidth problems on the network, the **frame rate** allowed to each viewer can be limited. Select the **Unlimited** radio button to allow the highest available frame rate or select the **Limited to...** radio button and enter a value (1-30) fps in the field.

Overlay Settings

Use these settings to include an text, date, and time as overlay. Click for information on available options.

Preview

For a preview of the image before saving, select video format and **Open**. When satisfied with the settings, click **Save**.



H.264

GOV Settings

The GOV structure describes the composition of the video stream and setting the GOV-length to a higher value saves considerably on bandwidth.

Bit Rate Control

The bit rate type can be set as **Variable Bit Rate** (VBR) or **Constant Bit Rate** (CBR). VBR adjusts the bit rate according to image complexity, using up more bandwidth for increased activity in the image, and less when the monitored area is quiet.

CBR allows you to set a fixed **Target bit rate** that consumes a predictable amount of bandwidth. As the bit rate would usually need to increase for increased image activity, but in this case cannot, the frame rate and image quality are affected negatively. To partly compensate for this, it is possible to prioritize either the frame rate or the image quality whenever the bit rate needs to be increased. Not setting a priority means the frame rate and image quality are equally affected.

Note:

To determine a reasonable bit rate, go to **Setup > Video > Video Stream > Image**, check the **Include** checkbox and enter the code **#b** in the **Include text**: field. The current bit rate will display as a text overlay on the **Live View** page.

To view the image stream while configuring the GOV settings and Bit rate control, select **Open...** under **Preview.**

MJPEG

Sometimes the image size is large due to low light or complex scenery. Adjusting the maximum frame size helps to control the bandwidth and storage used by the Motion JPEG video stream in these situations. Defining the frame size as **Unlimited** provides consistently good image quality at the expense of increased bandwidth and storage usage during low light. Limiting the frame size optimizes bandwidth and storage usage, but may give poor image quality. To prevent increased bandwidth and storage usage, the maximum frame size should be set to an optimal value.

Stream Profiles

There are 4 pre-programmed stream profiles available for quick set-up. These settings can be adjusted and new customized profiles can be created. Each profile has a descriptive name, describing its usage and/or purpose. The profiles can be accessed from the **Live View** page.

- To add a new stream profile, click **Add** to bring up the Stream Profile Settings panel.
- Choose a descriptive name and enter a description for your profile.
- Choose the form of **Video encoding** you wish to use from the drop-down list:

  H.264 – Also known as MPEG-4 Part 10. This is the new generation compression standard for digital video. This function offers higher video resolution than Motion JPEG or MPEG-4 at the same bit rate and bandwidth, or the same quality video at a lower bit rate.

  Motion JPEG – Delivers a high quality video stream, from which individual images can be extracted and saved.
- **Copy** an existing stream profile to your system and rename the copy
- **Modify** an existing stream profile based on the light situation and motion to be captured by your video encoder. See *Stream Profiles,* on page 13 for more information.
- Highlight the stream profile you wish to remove, then click **Remove** to remove it from the list.

Camera Settings

This page provides access to the advanced image settings for the AXIS Q7406.

Image Appearance

Color level – Select an appropriate level by entering a value in the range 0-100. Lower values mean less color saturation, whilst the value 100 gives maximum color saturation.

Brightness – The image brightness can be adjusted in the range 0-100, where a higher value produces a brighter image.

Contrast – Adjust the image's contrast by raising or lowering the value in this field.

Video Input

Offset Adjustments – Entering values in these fields changes the horizontal and vertical synchronization for the image. This can be used to eliminate any black border surrounding the image.

Be careful to only use low values, no more than 1-3, as higher values may put the image out of sync.

4CIF de-interlacing – is used to improve video stream image quality from analog devices. Select Adaptive Interpolation from the drop down list for best image quality. For improved image quality that is not as processor intensive, select Blending. If de-interlacing is not necessary select None.

Overlay Image

To use an overlay image in the AXIS Q7406 Video Encoder, it must be selected from the drop-down list of available images. The overlay (e.g. a logo) is then displayed in the video image.

To use your own image, first upload it to the AXIS Q7406 Video Encoder by entering the name of the file in the field provided, or by clicking the Browse button and locating it. Then click the **Upload** button.

Once your own image has been uploaded it will be available for selection from the drop-down list.

For more information please check the online help .

Privacy mask

Privacy masks are up to 3 configurable areas of solid color that allow concealment of parts of the image that are not to be viewable. Privacy masks cannot be bypassed via the AXIS VAPIX HTTP API.

Privacy Mask List

The Privacy Mask List shows all the masks that are currently configured in AXIS Q7406 and if they are enabled.

Add/Edit Mask

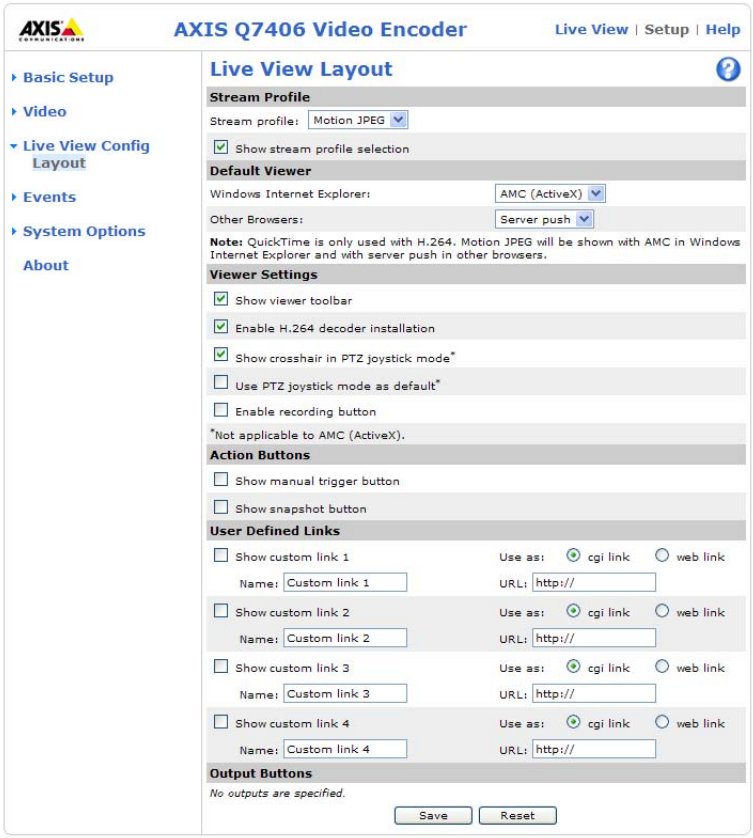
To define a new mask:

1. Click **Add** and place the box over the desired area to conceal.
2. Choose a color, black, white, gray or red for the box from the drop-down list Privacy mask color
3. Enter a descriptive name in the **Mask name** field.
4. Click **Save**.

To edit a privacy mask, select it and reshape, move or change color as needed.

Live View Config

Layout



Stream Profile

From the **Stream Profile** drop-down list, select the stream profile that is to be used for the **Live View** page. Listed are the standard stream profiles as well as the ones created under **Video > Stream Profiles**. See the online help files on this page for more information.

Default Viewer

From the drop-down lists, select the default method for viewing video images for your browser. The video encoder attempts to show the video images in the selected video format and viewer. If this is not possible, the video encoder overrides the settings and selects the best available combination.

Browser	Viewer	Description
Windows Internet Explorer	AMC	Recommended viewer in Windows Internet Explorer (H.264/Motion JPEG).
	QuickTime	H.264 only.
	Java applet	A slower imaging alternative to AMC. Requires one of the following installed on the client: • JVM (J2SE) 1.4.2 or higher • JRE (J2SE) 5.0 or higher
	Still image	Displays still images only. Hit the Refresh button in your browser to view a new image.
Other browsers	Server Push	Recommended viewer for other browsers (Motion JPEG).
	QuickTime	H.264 only.
	Java applet	A slower imaging alternative to Server Push (Motion JPEG only).
	Still image	Displays still images only. Hit the Refresh button in your browser to view a new image.

Viewer Settings

Check the **Show viewer toolbar** box to display the AXIS Media Control (AMC) or the QuickTime viewer toolbar under the video image in your browser.

The administrator can disable the installation of the **H.264 decoder** included with AMC. This is used to prevent the installation of unlicensed copies. Further decoder licenses can be purchased from your Axis dealer.

Check the **Enable recording button** to enable recording from the **Live View** page.

Action Buttons

The **Show manual trigger button** can be used to manually trigger and stop an event from the **Live View** page. See *Event Configuration,* on page 24.

Check the **Show snapshot button** to save a snapshot from the video stream. This button is mainly intended for use with browsers other than Internet Explorer, or when not using AXIS Media Control (AMC) to view the video stream. AMC for Internet Explorer provides its own snapshot button.

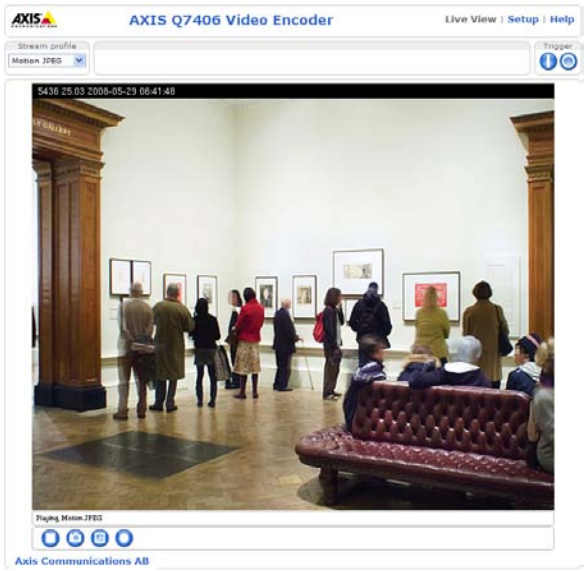
Time limit - set the desired length of the recording in hours/minutes/seconds.

User Defined Links

User defined links can be CGI links or web links. Once configured, the link(s) appear on the **Live View** page.

To set up a web link, select the **Use as web link** radio button, enter a descriptive name and enter the URL in the provided field. Click **Save** and the link appears in the **Live View** page.

User defined CGI links can be used to issue HTTP API requests, such as PTZ commands.



user defined link

Example:

1. Check **Show Custom Link 1**.
2. Enter a descriptive name, such as "Start continuous pan".
3. Select the **Use as cgi link** radio button and enter the cgi link in the field:

http://192.168.0.125/axis-cgi/com/ptz.cgi?continuouspantiltmove=30,-30

4. Check **Show Custom** Link 2.
5. Enter a descriptive name, such as "Stop continuous pan".
6. Select the **Use as cgi link** radio button and enter the cgi link in the field:

http://192.168.0.125/axis-cgi/com/ptz.cgi?continuouspantiltmove=0,0

These links appear in the web interface and can be used to control the Axis video encoder.

For more information on the Axis HTTP API, see the Support/Developer pages on the Axis Web site at http://www.axis.com

Please use the online help files for more information.

Output Buttons

The output buttons are used to manually activate the output from the **Live View** page, for example, switching a light on and off. There are two options to activate the output:

- Pulse button - activates the output for a defined period
- Active/Inactive - displays two buttons (on/off)

Pan Tilt Zoom

Installing PTZ devices

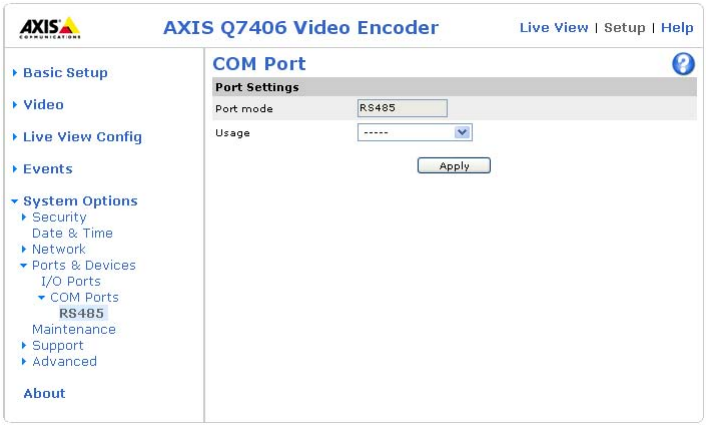
AXIS Q7406 supports several PTZ devices. Please see www.axis.com for a complete list of supported devices, and to obtain the correct driver.

If the AXIS Q7406 is mounted into an AXIS Q7900, one PTZ device can be connected to each of the six video channels.

If the AXIS Q7406 is mounted into an AXIS 291, video input 1 on the AXIS Q7406 supports several Pan Tilt Zoom (PTZ) devices. PTZ devices can also be used on video inputs 2-6, by creating an internal connection to them from video input 1. For further information see *Using PTZ on video inputs 2-6 (AXIS 291 1U Video Server Rack)*, on page 22.

Follow the instructions below to install a PTZ device:

1. Using an appropriate cable, connect the device to your selected port (RS-422 or RS-485). These ports are available via the I/O terminal connector. See *Pin assignments for the I/O Connector of the AXIS 291 1U Video Server Rack*, on page 39 and *Pin assignments for the I/O Connector of the AXIS Q7900 Rack*, on page 40 for more information.
2. Go to **Setup > System Options > Ports & Devices**.



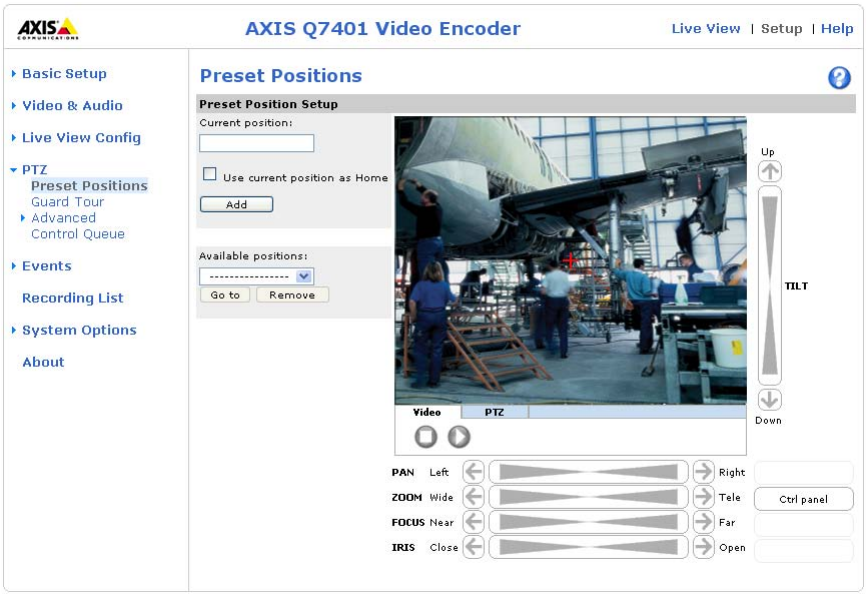
3. Select **Pan Tilt Zoom** from the **Usage** drop-down list.
4. Click **Upload** to install a PTZ driver**.**
   (PTZ drivers are available from the Axis Web site at www.axis.com)
5. Click **Port Options...** to modify the port settings. The default values correspond to the values specified by the PTZ driver.
6. From **System Options > Ports & Devices**, select the port configured for PTZ and then select the video source to use with the device.
7. If required, click the **Advanced Options** button to make further settings and see the online help .

Note:

Advanced users and application developers can also use the Axis Application Programming Interface and HTTP specification for generic control of PTZ devices using CGI commands or a TCP/IP client. Please refer to the Axis website at www.axis.com for further information.

PTZ configuration

Once PTZ has been installed for the AXIS Q7406, **PTZ Configuration** now appears in the menu to the left along with the following sub menus:



Preset positions

A preset position is a pre-defined camera view than can be used to quickly move the camera to a specific location.

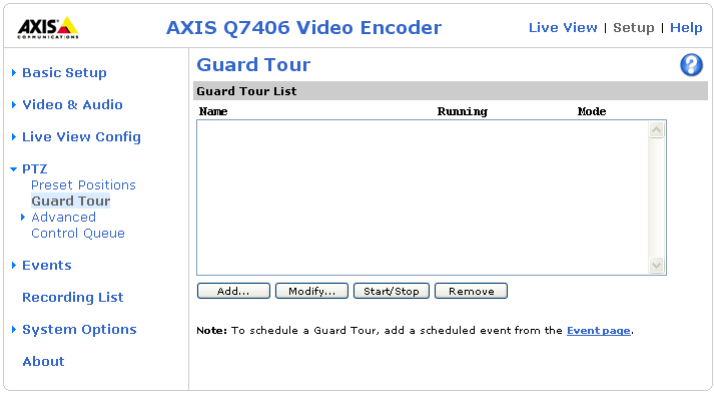
From **Preset Position Setup**, use the Pan, Tilt and Zoom (PTZ) controls to steer the camera to the required position. When satisfied with the camera's position, enter a descriptive name. The camera position, iris and focus settings are then saved as a preset position.

The position can be assumed at any time, by selecting the preset's name from the **Preset positions** drop-down list. Preset positions can be selected in the **Live View** page; they can be selected as an action when an event is triggered as part of a **Guard Tour**.

One position can be set as the Home position, which is readily accessible by clicking the box beside **Use current position as Home**. The position's name will then have (H) added to the end, for example, Office Entrance (H).

Guard tour

A guard tour moves between chosen **Preset Positions**, one-by-one, in a pre-determined order or at random, and for configurable time periods. The guard tour sequence will keep running, after the user has logged off or closed the browser.



Advanced

Device Settings - The device settings window is for driver specific settings, so the appearance of this window can vary depending on the driver installed. Options that can be configured include: **Driver Specific Settings for Video Source 1**, **Mechanical Limits for Moving Video Source 1**, **Light Control for Video Source 1**, and **Extended Driver Specific Settings for Video Source 1**.

Ctrl Panel - The **Panel View Settings** window contains tools for creating and saving short command buttons that are located under the **Control panel**. These buttons provide direct access to various built-in auxiliary commands provided by the PTZ driver and are displayed in the PTZ Panel.

Limits - Define the pan, tilt, zoom and focus limits for the video encoder. Movements to the left and right, up and down can be restricted to narrow the area under surveillance. The near focus limit can be set to avoid focusing on objects too close to the camera.

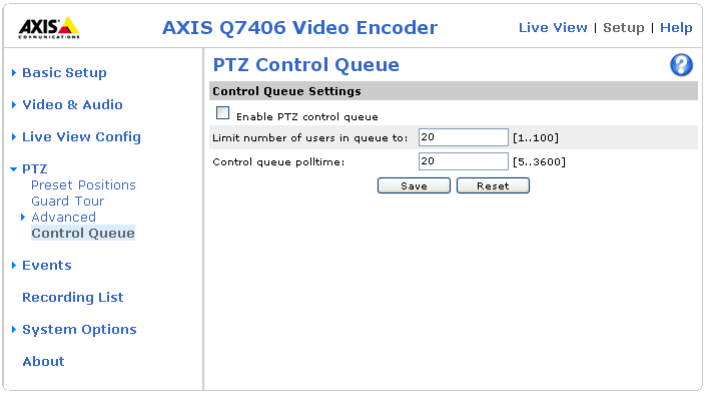
Note:

To be able to set limits, the driver needs to be an "absolute" driver.'

OSD Menu - If the PTZ unit supports an internal configuration menu, this can be accessed using the On-Screen Display (OSD). Configure the analog camera by opening and navigating through its internal menu in this display.

PTZ control queue

Use the PTZ control queue window to enable and disable PTZ queueing. This window allows you to set up a queue for viewers wanting to access the video encoder, and limits the number of viewers and the length of time each viewer can access and control the PTZ unit. For more information on how to set up the control queue, please see the online help .



Note also that a viewer who belongs to a group (see *Security*, on page 29) with a higher PTZ priority can go before other users in the queue and take control of the video encoder.

The order of priority for taking control of the queue is as follows:

1. **Administrators** - An administrator takes over PTZ control regardless of who is first in queue. The administrator will be removed from the queue 60 seconds after their last PTZ control command.
2. **Event** - The AXIS Q7406 can be set up to take control of the queue and move to a specific position for 20 seconds when triggered by an alarm. The event will immediately be placed first in the queue, except when an administrator is in control. For more information, see *Triggered Event*, on page 25.
3. **Operator** - Same as administrator, but with lower priority.
4. **Guard Tour** - A guard tour has PTZ control for an indefinite period of time. It may be overridden by an Operator, Event or administrator. Guard Tour will resume when higher priority groups leave the queue. For more information see *Guard tour*, on page 19.
5. **Viewer** - Multiple viewers must wait for their turn. The viewer has 60 seconds of PTZ control before control is passed to the next viewer in queue.

Note:

To identify the different users in the viewer group, cookies must be enabled on the client.

PTZ controls

If the video encoder has been appropriately configured, the **Live View** page displays the controls available for the installed Pan Tilt Zoom (PTZ) device. The administrator can enable/disable the controls for specified users.

The controls shown depends on the make and model of PTZ device. The most common controls are:

- the Pan bar - moves the camera to the right and left
- the Tilt bar - tips the camera up and down
- the Zoom bar - zooms the view in and out. Note that this is only available if the camera is fitted with a zoom lens
- the Iris bar - adjusts the brightness of the image

Clicking on the bars themselves or on the arrows at the end of the bars moves the camera to a new position. The type of movement and the location of this new position depends on the type of PTZ driver.

When controlling the camera using a **relative** PTZ driver (see the bars in the illustration above) the new position is relative to the previous position, for example, left of, below, or above. Clicking the bar further from the center results in a larger movement.

In contrast, when using an **absolute** driver, each position on the bar (see right) represents a defined position in the device's range of movement, with the center of the bar representing the point midway between the two extremes of movement.

Clicking a position directly on the bar moves the camera directly to the new position in one smooth movement. Clicking on the arrows at the ends of a bar causes an incremental change.

Using CGI links to control PTZ devices

User-defined CGI links on the **Live View** page can be used to issue HTTP API requests, such as PTZ commands. These links are configured in the **Live View Layout** settings, see *Live View Config*, on page 15.

PTZ control modes

The PTZ device can also be controlled using **click-in-image** movement, which has two different types of navigation - **Center** and **Joystick.**

Center mode means that when clicking in the image, the camera view centers on the absolute position that was clicked.

Joystick mode moves the camera in the direction of the mouse pointer. By clicking and holding the mouse button down in the image, the PTZ device moves the camera in that direction, relative to the center of the image. The farther from the center the image is clicked, the greater the movement. The camera stops moving when the button is released.

Note:
There is also joystick support in AXIS Media Control (AMC).

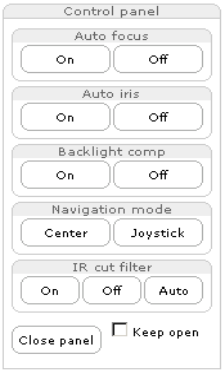
Control panel

The focus and iris (image brightness) can be adjusted manually by using the control bars, or they can be set for automatic adjustment, by clicking the **Auto iris** and **Auto focus** buttons.

Note:
These buttons appear only if the PTZ driver installed supports them.

To access the **Auto iris** and **Auto focus** buttons, click on the **Control panel** button. The menu to the right will then appear in the upper left hand corner of the screen.

There are also driver specific shortcuts that can appear in the Control Panel. In the screen to the right, a driver has been installed that brings up the **Wiper** shortcut button, which allows the user to configure and use a windshield wiping action with the video encoder.



Using PTZ on video inputs 2-6 (AXIS 291 1U Video Server Rack)

Although the AXIS Q7406 only supports an RS-485 port on video input 1 if it is mounted into an AXIS 291 1U Video Server Rack, it is still possible to use PTZ devices on video inputs 2-4 by creating virtual connections to these inputs from video 1 (See *RS-485 Connector (AXIS 291 1U),* on page 38). To do this, follow these steps:

1. Configure PTZ on video input 1 and install the required PTZ driver. This step is always required, whichever video input you intend to use for PTZ, and is described in detail in *Installing PTZ devices*. Refer also to *RS-485 Connector (AXIS 291 1U),* on page 38.
2. Repeat this procedure and install the same device driver on the other video input(s) you wish to use PTZ on.

3. Enter the same Authentication key as configured for video input 1. This will prevent unauthorized access to the RS-485 port.

PTZ devices on inputs 2-6 are configured in the same way as a device on video input 1. See *PTZ configuration*.

Applications

Application Packages

The Applications feature allows you to upload third party applications for use on this device. Listed under **Applications** > **Packages** are the applications that have already been installed. Click on the name to view the menu options - **Settings**, **License** and **About**.

Settings - This is dependent on the application.

License - Once uploaded some applications need a license to run, and a license code is required for the uploaded application. If there is an Internet connection in the camera, **Automatic Installation** appears in the web page. If there is no Internet connection to the camera, go to www.axis.com to acquire a License key file. You will need a license code and the device's serial number to receive a license key.

About - Details support for this application. To upload an application, browse to the package and click **Upload Package**.

Installed Applications - A list of installed applications with information about the version, and the vendor; the status of the application (running or not running), and information about the license (if installed).

Start/Stop - Start or stop the application.

Remove - To delete an application, select it and click **Remove**.

Log - To generate a log of the application happenings, select an application and click **Log**. This log is helpful when requesting support from the application's vendor.

Note:

It is recommended that you do not run more than one application at a time. Also do not run an application when the motion detection feature is active.

Event Configuration

An **event** or **Event Type** in the camera triggers actions when activated. An event type is a set of parameters that defines the actions. A common event type is an alarm that causes the camera to upload images. Many event types use an **Event Server**, to receive uploaded images.

This section describes how to configure the camera to perform certain actions when events occur.

Definitions

Event type	A set of parameters describing how and when the camera performs certain actions
Triggered Event - see page 25	An event that is started by some sort of signal, for example, an external device such as a door switch, motion detection, or system event.
Scheduled Event - see page 26	Pre-programmed time period(s) during which an event will run.
Action	This occurs when the event runs, for example, uploading of images to an FTP server, or email notification.

Event Servers

Event Servers are used to receive uploaded image files and/or notification messages. To set up Event Server connections in your camera, go to **Setup > Event Configuration > Event Servers** and enter the required information for the required server type.

Server type	Purpose	Information required
FTP Server	• Receives uploaded images	• Descriptive name of your choice • Network address (IP address or host name) • User Name and Password
HTTP Server	• Receives notification messages • Receives uploaded images	• Descriptive name of your choice • URL (IP address or host name) • User Name and Password
TCP Server	• Receives notification messages	• Descriptive name of your choice • Network address (IP address or host name) • Port number

For details on each setting, see the online help available from each web page.

When the setup is complete, the connection can be tested by clicking the **Test** button (the connection test takes approximately 10 seconds).

Event Types

An **Event Type** describes how and when the camera performs certain actions.

AXIS Q7406 Video Encoder
Live View | Setup | Help
Basic Setup
Video & Audio
Live View Config
Events
Instructions
Event Servers
Event Types
Camera Tampering
Motion Detection
Port Status
Recording List
System Options
About
Event Types
Event Type List
Name Enabl. Priority Trig./Sched. Actions*
Main door Yes Low Input ports O
New Event Yes Normal Audio O
Server room Yes Normal Time frame Hu
Add triggered... Add scheduled... Copy Modify... Remove
* Fu=FTP upload, Hu=HTTP upload, Eu=Email upload, O=Output port, En=Email notification, Hn=HTTP notification, Tn=TCP notification, Rec=Record to disk, P=PTZ preset, G=Guard Tour

Example: If somebody passes in front of a camera and an event has been configured to detect and respond to motion, the camera can record and saves images to an FTP server, and can send a notification e-mail to an e-mail address. Images can be sent as e-mail attachments.

Triggered Event

A triggered event could be activated by:

- a push button connected to the camera's input port
- a manually activated action, such as from an action button in the web interface
- detected movement in a configured motion detection window
- on restart (reboot), after power loss
- camera tampering
- video loss
- rack monitor*

* the rack monitor applies to the first channel on the first slot and will trigger on a malfunctioning fan or power supply or if the temperature is too high.

How to set up a triggered event

The following example describes how to set up the camera to upload images when the main door is opened.

1. Click **Add triggered...** on the **Event Types** page. The **Triggered Event Type Setup** page appears.
2. Enter a descriptive **Name** for the event, such as Main door open.
3. Set the **Priority** - High, Normal or Low (see the online help).
4. Set the **Respond to Trigger...** parameters to define when the event is active, for example, after office hours.
5. Select the trigger alternative from the **Triggered by...** drop-down list. For example, select Input ports, for a sensor connected to the door.
6. Set the **When Triggered...** parameters, that is, define what the camera will do if the main door is opened - upload images to an FTP server or send an e-mail notification.
7. Click **OK** to save the event in the Event Types list.

Please see the online help for descriptions of each available option.

Note:

Up to 10 event types can be configured in the camera, and up to four of these can be configured to upload images. File names can be formatted according to specific requirements. See File Naming & Date/Time Formats online help.

Pre-trigger and Post-trigger buffers

This function is very useful when checking to see what happened immediately before and/or after a trigger, for example, 30 seconds before and/or after a door was opened. Check the **Save stream** checkbox under **Event Types > Add Triggered... > When Triggered...** to view the options. All uploaded images are JPEG images.

Include pre-trigger buffer - images stored internally in the server from the time immediately preceding the trigger. Check the box to enable the pre-trigger buffer, enter the desired length of time and specify the required image frequency.

Include post-trigger buffer - contains images from the time immediately after the trigger. Configure as for pre-trigger.

Notes

- Pre-trigger and Post-trigger buffers will be lost if the connection to the event server fails.
- The maximum length of the pre-/post-buffer depends on the video image size and selected frame rate.
- If the pre- or post-buffer is too large for the camera's internal memory, the frame rate is reduced and individual images may be missing. If this occurs, an entry is created in the unit's log file.

Continue image upload (unbuffered) - enables the upload of video images for a fixed length of time. Specify the length of time for the uploaded recording, in seconds, minutes or hours, or for as long as the trigger is active. Finally, set the desired image frequency to the maximum (the maximum available) or to a specified frame rate. The frame rate will be the best possible, but might not be as high as specified, especially if uploading via a slow connection.

Scheduled Event

A **Scheduled event** can be activated at preset times, in a repeating pattern on selected weekdays.

Configuration example:

1. Click **Add scheduled...** on the **Event Types** page.
2. Enter a descriptive **Name** for the event, such as Scheduled e-mail upload.
3. Set the **Priority** (High, Normal or Low).
4. Set the **Activation Time** parameters (24h clock) for the event - start on Sundays at 13.00 with a duration of 12 hours.
5. Set the **When Activated...** parameters, (what the camera would do at the specified time) for example, send uploaded images to an e-mail address.
6. Click **OK** to save the Event in the Event Types list.

Please see the online help for descriptions of each available option.

Camera tampering

The camera tampering application generates an alarm whenever the camera is repositioned, or when the lens is covered, sprayed, or severely defocused.

First, you must create an event, see *How to set up a triggered event*, on page 25, for the camera to send an alarm.

Settings

The **Minimum duration** parameter sets the minimum tampering period, that is an alarm will not be triggered until this period has elapsed, even if the tampering conditions are otherwise met. This can help prevent false alarms for known conditions that affect the image.

If the camera lens is sprayed or covered so that the camera live view becomes dark, it will not be possible to distinguish this situation from other situations where the same effect is seen, such as when lighting conditions change.

When the **Alarm for dark images** parameter is enabled, alarms are generated for all cases where the lights are either dimmed or turned off, or if the lens is sprayed, covered, or rendered severely out of focus. If not enabled, no alarm will be sent.

After you define these settings, click **Save**.

Motion Detection

Motion detection is used to generate an alarm whenever movement occurs (or stops) in the video image. A total of 10 Include and/or Exclude windows can be configured.

- **Included** windows target specific areas within the whole video image
- **Excluded** windows define areas within an Include window that should be ignored (areas outside Include windows are automatically ignored)

Once configured, the motion detection windows appear in the list of available triggers, for triggering events. See *How to set up a triggered event*, on page 25.

Note:

Using the motion detection feature may decrease the camera's overall performance.

Configuring Motion Detection

1. Click **Motion Detection** in the **Event Configuration** menu.
2. Click the **Add Window** button.
3. Select the **Include** or **Exclude** option to define an Include or Exclude window, and enter a descriptive name in the field below.
4. Adjust the size (drag the bottom right-hand corner) and position (click on the text at the top and drag to the desired position) of the active window.
5. Adjust the **Object Size**, **History** and **Sensitivity** profile sliders (see table below for details). Any detected motion within an active window is then indicated by red peaks in the **Activity** window (the active window has a red frame).
6. Click **Save**.

> To exclude parts of the Include window, select the **Exclude** option and position the Exclude window as required, within the Include window.

Please see the online help for descriptions of each available option.

	Object Size	History	Sensitivity
High level	Only very large objects trigger motion detection	An object that appears in the region will trigger the motion detection for a long period	Ordinary colored objects on ordinary backgrounds will trigger the motion detection
Low level	Even very small objects trigger motion detection	An object that appears in the region will trigger motion detection for only a very short period	Only very bright objects on a dark background trigger motion detection
Default value	Low	High	High

Examples:

- Avoid triggering on small objects in the video image by setting the **object size** level to high.
- To reduce the number of triggers if there is a lot of movement during a short period of time, select a high **history** level.
- To only detect flashing light, select low **sensitivity**. In other cases, a high **sensitivity** level is recommended.

Port Status

Under **Event Configuration > Port Status** there is a list showing the status for the camera's input and output. This is for the benefit of **Operators** who have no access to the System Options section.

Example: If the Normal state for a push button connected to an input is set to **Open circuit –** as long as the button is not pushed, the state is **inactive**. If the button is pushed, the state of the input changes to **active**.

System Options

Security

Users

User access control is enabled by default. An administrator can set up other users, by giving these user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the **Live View** page, as described below:

The **user list** displays the authorized users and user groups (levels):

Viewer	Provides the lowest level of access, which only allows access to the **Live View** page.
Operator	An operator can view the **Live View** page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has unrestricted access to the Setup tools and can determine the registration of all other users.

HTTP/RTSP Password Settings – Select the type of password to allow. You may need to allow unencrypted passwords if there are viewing clients that do not support encryption, or if you recently upgraded the firmware and the existing clients do support encryption, but need to log in again, and be configured to use this functionality.

User Settings – Check the relevant box to enable **anonymous viewer login –** allows any viewer direct access to the **Live View** page.

Before using the AXIS Q7406, there are certain settings that should be made, most of which require Administrator access privileges. These settings can be quickly accessed through Basic Setup in the menu. All settings are also available from the standard menu. Basic Setup is enabled by default but can be disabled and removed from the menu, by deselecting the Enable **Basic Setup** box option.

IP Address Filter

Enable IP Address Filtering to allow or deny access to the video encoders**.** Once enabled, the IP addresses in the list are allowed or denied access according to the choice made in the drop-down list **Allow/Deny the following IP addresses.**

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses). The users from these IP addresses need to be specified in the user list with the appropriate access rights. This is done from **Setup > System Options > Security > Users**.

HTTPS

The video encoders support encrypted browsing using HTTPS.

A **self-signed certificate** can be used until a Certificate Authority-issued certificate has been obtained. Click the **Create self-signed Certificate** button to install a self-signed certificate. Although self-signed certificates are free and offer some protection, true security is only implemented after the installation of a signed certificate issued by a certificate authority.

A signed certificate can be obtained from an issuing Certificate Authority by clicking the **Create Certificate Request** button. When the signed certificate is returned, click the **Install signed certificate** button to import the certificate. The properties of any certificate request currently resident in the camera or installed can also be viewed by clicking the **Properties...** button. The HTTPS Connection Policy must also be set in the drop-down lists to enable HTTPS in the camera.

For more information, please refer to the online help.

IEEE 802.1X

IEEE 802.1X is a standard for port-based Network Admission Control providing secure authentication of wired and wireless network devices. IEEE 802.1X is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1X, devices must authenticate themselves. The authentication is performed by a

third-party entity called an authentication server, typically a RADIUS server, examples of which are FreeRADIUS and Microsoft Internet Authentication Service.

In Axis implementation, the network device and the authentication server authenticate themselves with the help of digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). The certificates are provided by an Certification Authority (CA). You need:

- a CA certificate to validate the identity of the authentication server
- a CA-signed client certificate and a private key to authenticate the network device.

To allow the network device to access a network protected by IEEE 802.1X:

1. Obtain a CA certificate, a client certificate and a client private key (contact your network administrator).
2. Go to Setup > System Options > Security > IEEE 802.1X and upload the CA certificate, the client certificate and the client private key.
3. Under SETTINGS, select the EAPOL version, provide your EAP identity and private key password.
4. Check the box to enable IEEE 802.1X and click Save.

Certificates

Certificates	
CA Certificate	The CA certificate is used to validate the identity of the authentication server. Enter the path to the certificate directly, or locate the file using the Browse button. Then click Upload. To remove a certificate, click Remove.
Client Certificate Client private key	The client certificate and private key are used to authenticate the network device. They can be uploaded as separate files or in one combined file (e.g. a PFX file or a PEM file). Use the Client Private Key field if uploading one combined file. For each file, enter the path to the file, or locate the file using the Browse button. Then click Upload. To remove a file, click Remove.
Settings	
EAPOL Version	Select the EAPOL version (1 or 2) as used in your network switch.
EAP Identity	Enter the user identity (maximum 16 characters) associated with your certificate.
Private Key Password	Enter the password (maximum 16 characters) for the private key.
Enable IEEE 802.1X	Check the box to enable the IEEE 802.1X protocol.

Date & Time

Current Server Time – displays the current date and time (24h clock). The time can be displayed in 12h clock format in the overlay (see below).

New Server Time – select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select the **Automatically adjust for daylight saving time changes**.

From the **Time Mode** section, select the preferred method to use for setting the time:

- **Synchronize with computer time** - sets the time from the clock on your computer.
- **Synchronize with NTP Server** - the camera will obtain the time from an NTP server on a regular basis.
- **Set manually** - this option allows you to manually set the time and date.

Note:

If using a host name for the NTP server, a DNS server must be configured under **TCP/IP** settings.
See **Network > Basic TCP/IP Settings** below.

Date & Time Format Used in Images - specify the formats for the date and time (12h or 24h) displayed in the video streams.

Use the predefined formats or use your own custom date and time formats. See **Advanced File Naming & Date/Time Formats** in the online help for information on how to create your own date and time formats.

Network

Basic TCP/IP Settings

AXIS Q7406 support both IP version 4 and IP version 6. Both versions may be enabled simultaneously, and at least one version must always be enabled. When using IPv4, the IP address for the camera can be set automatically via DHCP, or a static IP address can be set manually. If IPv6 is enabled, the video encoders receive an IP address according to the configuration in the network router. There is also the option of using the AXIS Internet Dynamic DNS Service. For more information on setting the IP address, please see the online help .

Network Settings – Click the **View** button for an overview of the IP configuration of the video encoder.

IPv4 Address Configuration – Check this box to enable IPv4.

Obtain IP address via DHCP – Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.

Note:

DHCP should only be enabled if using dynamic IP address notification (see below), or if your DHCP server can update a DNS server, which then allows you to access the AXIS Q7406 by name (host name). If DHCP is enabled and you cannot access the unit, you may have to reset it to the factory default settings and then perform the installation again.

Use the following IP address – To use a static IP address for the AXIS Q7406, check the radio button and then make the following settings:

- IP address - Specify a unique IP address for your AXIS Q7406. (To check if the IP address you intend to use is available or not, click the Test button)
- Subnet mask - Specify the mask for the subnet the AXIS Q7406 is located on
- Default router - Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

IPv6 Address Configuration – Check the box to enable IPv6. Other settings for IPv6 are configured in the network router.

Services – Enable ARP/Ping setting of IP address - The IP address can be set using the ARP/Ping method, which associates the unit's MAC address with an IP address. Check this box to enable the service. Leave disabled to prevent unintentional resetting of the IP address.

Notes:

- The ARP/Ping service is automatically disabled two minutes after the unit is started, or as soon as an IP address is set.
- Pinging the unit is still possible when this service is disabled.

Enable AVHS – AXIS Video Hosting System (AVHS) in conjunction with an AVHS service provides easy and secure Internet access to live and recorded video accessible from any location. For more information and help to find a local AVHS Service Provider please go to www.axis.com. If AVHS is not to be used this option can be disabled.

One-click enabled - Press the camera's control button (see *Overview*, on page 4) to connect to an AVHS service over the Internet. Once registered the camera stays connected to the AVHS service. If the camera is not registered within 24 hours after the button is pressed, the camera will disconnect from the AVHS service.

Always - The camera will constantly attempt to connect to the AVHS service over the Internet. Once registered the camera will stay connected to the service. This option can be used when the camera is already installed and it is not convenient to use the one-click installation.

AXIS Internet Dynamic DNS Service - Use the AXIS Internet Dynamic DNS service to assign a host name for easy access to your video encoder (requires Internet access).

Click **Settings...** to register the camera with the Axis Internet Dynamic DNS service, or to modify the existing settings (requires access to the Internet). The domain name currently registered at the Axis Internet Dynamic DNS service for your product can at any time be removed.

For more information, please refer to the online help .

Advanced TCP/IP Settings

DNS Configuration – DNS (Domain Name Service) provides the translation of host names to IP addresses on your network.

Obtain DNS server address via DHCP - automatically use the DNS server settings provided by the DHCP server. Click the **View** button to see the current settings.

Use the following DNS server address - enter the desired DNS server by specifying the following:

Domain name - enter the domain(s) to search for the host name used by the video encoders. Multiple domains can be separated by semicolons (;). The host name is always the first part of a Fully Qualified Domain Name, for example, **myserver** is the host name in the Fully Qualified Domain Name **myserver.mycompany.com** where mycompany.com is the Domain name.

DNS servers - enter the IP addresses of the primary, and secondary DNS servers.

Note:
This is not mandatory with regard to secondary DNS servers.

NTP Configuration – Obtain NTP server address via DHCP - select this radio button option to automatically look up and use the NTP server settings as provided by DHCP. Click the **View** button to see the current settings.

Use the following NTP server address – to create manual settings, check this radio button and enter the host name or IP address of the NTP server.

Host Name Configuration – The video encoders can be accessed using a host name, instead of an IP address. The host name is usually the same as the assigned DNS Name.

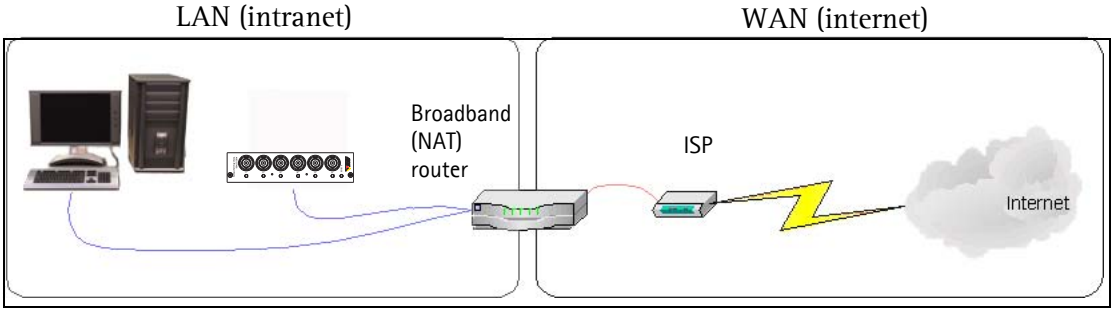
For more information, please see *Security*, on page 29.

Link-Local IPv4 Address – This is enabled by default and assigns the video encoders an additional IP address for use with UPnP™. The camera can have both a Link-Local IP and a static/DHCP-supplied IP address at the same time - these will not affect each other.

HTTP and HTTPS – The default HTTP/HTTPS port numbers (80 and 443 respectively) can be changed to any port within the range 1024-65535. This is useful for simple security port mapping, for example.

NAT traversal (port mapping) for IPv4 – A broadband router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the "outside", that is, the Internet. Security on the private network (LAN) is increased since most broadband routers are pre-configured to stop attempts to access the private network (LAN) from the public network/Internet.

Use **NAT traversal** when your video encoders are located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the camera.



Notes:

- For NAT traversal to work, this must be supported by the broadband router.
- The broadband router has many different names: "NAT router", "Network router", Internet Gateway", "Broadband sharing device" or "Home firewall" but the essential purpose of the device is the same.

Enable/Disable - when enabled, the video encoders attempt to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the camera (see **System Options > Network > UPnP**).

Use manually selected NAT router - select this option to manually select a NAT router and enter the IP address for the router in the field provided.

If a router is not manually specified, the video encoders automatically search for NAT routers on your network. If more than one router is found, the default router is selected.

Alternative HTTP port - select this option to manually define an external HTTP port. Enter the port number in the field provided. If no port is entered here a port number is automatically selected when NAT traversal is enabled.

Notes:

- An alternative HTTP port can be used/be active even if NAT traversal is disabled. This is useful if your NAT router does not support UPnP and you need to manually configure port forwarding in the NAT router.
- If you attempt to manually enter a port that is already in use, another available port is automatically selected.
- When the port is selected automatically it is displayed in this field. To change this enter a new port number and click Save.

FTP – The FTP server running in the video encoders enables the upload of new firmware, and user applications. Check the box to enable the service.

RTSP – The RTSP protocol allows a connecting client to start an H.264 stream. Check the box to enable the server and enter the RTSP port number to use. The default setting is 554. Note that H.264 video streams will not be available if this service is not enabled.

SOCKS

SOCKS is a networking proxy protocol. The Axis video encoder can be configured to use a SOCKS server to reach networks on the other side of a firewall/proxy server. This functionality is useful if the video encoder is located on a local network behind a firewall, and notifications, uploads, alarms, and such need to be sent to a destination outside the local network (such as the Internet). See the online help for more information.

QoS (Quality of Service)

Quality of Service (QoS) guarantees a certain level of a specified resource to selected traffic on a network. Quality can be defined as a maintained level of bandwidth, low latency, and no packet losses. The main benefits of a QoS-aware network can be summarized as:

- The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
- Greater reliability in the network, thanks to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.

The QoS in Axis network video products marks the data packets for various types of network traffic originating from the product. This makes it possible for network routers and switches to reserve a fixed amount of bandwidth for these types of traffic. The video encoders mark the following types of traffic:

- video
- event/alarm
- management network traffic

QoS Settings – For each type of network traffic supported by your Axis network video product, enter a DSCP (Differentiated Services Codepoint) value. This value is used to mark the traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the router or switch the type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Note that DSCP values can be entered in decimal or hex form, but saved values are always shown in decimal.

For more information on Quality of Service, please see the Axis support web at www.axis.com/techsup

SMTP (email)

Enter the host names (or IP addresses) and port numbers for your primary and secondary mail servers in the fields provided, to enable the sending of notifications and image email messages from the camera to predefined addresses via SMTP.

If your mail server requires authentication, check the box for **Use authentication to log in to this server** and enter the necessary information. See the online help for more information.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices. Depending on the level of security required, select the version of SNMP to use. The three levels of security are:

- SNMP V1 - includes no security.
- SNMP V2c - uses very simple security. The community name can be specified as a password for read or read/write access to all supported SNMP objects. The community is the the group of network devices using SNMP.
- SNMP V3 - provides encryption and secure passwords. HTTPS must be enabled.

Traps for SNMP v1/v2/v3

Traps are used by the camera to send messages to a management system for important events or status changes. These settings are used with SNMP v1/v2. To activate trap reporting, enter the IP address of the management server, and choose the trap community to use when sending a trap message to the management system.

SNMP v3 is a more secure version providing encryption and secure passwords. To use SNMP v3, HTTPS must be activated. To use traps with SNMP v3 an SNMP v3 management application is needed.

See the online help for more information.

UPnP™

The video encoder includes support for UPnP™. UPnP™ is enabled by default, and the video encoder then is automatically detected by operating systems and clients that support this protocol.

RTP/H.264

These settings are the port range, IP address, port number (video), and Time-To-Live value to use for the video stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams. For more information, please see the online help .

Bonjour

The video encoders include support for Bonjour. When enabled, the camera is automatically detected by operating systems and clients that support this.

Ports & Devices

I/O Ports – the pinout, interface support and the control and monitoring functions provided by this connector are described in *Pin assignments*, on page 39.

COM Port – Selecting Pan Tilt Zoom enables the port to be used for controlling a connected PTZ device. Basic serial port settings can be adjusted by clicking the **Port Options** button.

The PTZ Driver Management section shows the name and version of the PTZ driver currently in use. To install a new driver, click the **Upload** button. PTZ drivers can be obtained from www.axis.com. Please note that using the wrong PTZ driver for a PTZ device may cause unwanted effects.

For more information please see the online help .

LED Settings

The Status indicator LED on the front of the camera can be set to flash at a configurable interval (or to not light up at all) when the unit is accessed. For a listing of all LED behavior, see *LED indicators*, on page 5, or the online help .

Maintenance

- **Restart** - the camera is restarted without changing any setting.
- **Restore** - the unit is restarted and most current settings are reset to factory default values. The settings that do not reset are:
    - the boot protocol (DHCP or static)
    - the static IP address
    - the default router
    - the subnet mask
    - the system time
    - 802.1X settings
- **Default** - the default button should be used with caution. Pressing this returns the camera's settings to the factory default values (including the IP address).

Upgrade Server – See *Upgrading the Firmware*, on page 42.

Support

The **Support Overview** page provides valuable information on troubleshooting and contact information, should you require technical assistance.

System Overview - is an overview of the camera's status and settings. Information that can be found here includes the camera's firmware version, IP address, security, event and image settings and recent log items. Many of the captions are also links to the proper **Setup page** to conveniently make adjustments in the camera's settings.

Logs & Reports - when contacting Axis support, please be sure to provide a valid Server Report with your query. The Access Log is automatically included in the server report.

Information - the **Logs,** the **Server Report** and the **Parameter List** may prove useful when troubleshooting a problem or when contacting the Axis support web.

System Log - Provides information about system events.

Access Log - The Access Log may be used for various purposes:

- Security - Tracking all access to your the camera. The access log lists the IP addresses, users and networking protocols used to access the camera.
- Simple web attraction tracker.
- System analysis and trouble shooting.

Server Report - Provides information about the server status and should always be included when requesting support.

Parameter List - Shows the unit's parameters and their current settings.

Connection List - Lists all clients that are currently accessing video. It is also used for system analysis and trouble shooting.

Configuration

From the drop-down lists, select the size and level of information to be added to the System and Access Log files.

The default information level for the Access Log is set to Critical & Warnings. However, in an error situation and when requesting support, set it to the lowest information level Critical & Warnings & Info.

For the Log Level for Email, select from the drop-down list the level of information to send as email and enter the destination email address.

Advanced

Scripting is an advanced function that enables you to customize and use scripts. This function is a very powerful tool.

Caution!

Improper use may cause unexpected behavior or even cause loss of contact with the unit. If a script does cause problems, reset the unit to its factory default settings. A backup file may be of use to return the unit to its latest configuration.

Axis strongly recommends that you do not use this function unless you understand the consequences. Note that Axis support does not provide assistance for problems with customized scripts.

For more information, please visit the Developer pages at www.axis.com/developer

File Upload - To use your own files (web pages and images) as custom settings, they must first be uploaded to the AXIS Q7406 video encoder. To do this, enter the name and path to the file in the field provided; or click the **Browse** button and select the file. Select the user level for the uploaded file. This helps you define user access to files. When the file is displayed correctly in the text field, click the **Upload** button. All uploaded files are shown in the list in the lower section of the page. To remove a file, check the box provided next to it and then click the **Remove** button.

Plain Config - this function is for the advanced user with experience of Axis video encoder configuration. All parameters can be set and modified from this page. Help is available from the standard help pages.

About

Here you can find basic information about your video encoder. You can also view third party software licenses.

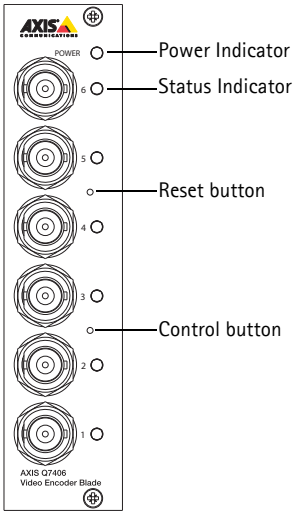
Resetting to the Factory Default Settings

This will reset all the parameters, in all 6 units (including all six IP addresses), to the factory default settings.

1. Press both the Reset button and Control button.
2. Release the Reset button and hold the Control button.
3. Keep the Control button pressed until the Power indicator turns green and the six Status indicators turn amber (this may take up to 15 seconds).
4. Release the Control button. When the Status indicators display green (which can take up to 1 minute) the process is complete and the video encoder has been reset.
5. Re-assign the IP addresses, using one of the methods described in this document.

To reset an individual unit to the original factory default settings, use the button provided in that unit's web interface. For more information, please see the online help.

Note: For other methods of setting the IP address, please refer to the product's Installation Guide that accompanies the product, or download a copy from www.axis.com



Unit connectors

DIP Switches – Each video input has a corresponding line termination DIP switch. Axis blade video encoders are supplied with the line termination enabled for each input; that is, with the DIP switches set to ON (up position).
To connect the video input in parallel with other equipment, disable the input termination by setting the corresponding DIP switch to OFF (down position). Failure to do so may affect the image quality negatively.

Bus Connector – This is the physical interface to the video encoder rack, providing power, network and the I/O terminal connector.

Control Button – This button is used to reset the video encoder to the factory default settings. See *Overview*, on page 4.

Reset Button – This button disconnects and reconnects power to the video encoder. See *Overview*, on page 4.

Video Inputs – The AXIS Q7406 supports 6 video sources (VIDEO 1 - VIDEO 6). Each video input is terminated using a coax/BNC connector. Physical connections made using 75 Ohm coaxial video cable have a recommended maximum length of 800 feet (250 meters).

I/O Terminal Connector(s) (AXIS 291 1U) – Provides the physical interface to 2 configurable input/outputs on channels 1-2, and 1 configurable input/output for channels 3-6. Video input 1 on each blade also provides an RS-485 interface, usually used for connecting Pan Tilt Zoom devices. See *Pin assignments*, on page 39 for pin assignment information.

I/O Terminal Connector(s) (AXIS Q7900) – Provides the physical interface for up to 12 input/outputs. See *Pin assignments*, on page 39 for pin assignment information.

RS-485 Connector (AXIS 291 1U) – The RS-485 COM Port supports several operational modes:

- Generic TCP/IP - enables the video server to receive status/data and send commands via TCP/IP (only for channel 1 in the 291 rack)
- Generic HTTP - enables the video server to receive status/data and send commands via HTTP
- Pan Tilt Zoom (PTZ) - for controlling a PTZ device. A PTZ device requires a driver for its function. Drivers can be obtained from www.axis.com. Please see *Installing PTZ devices*, on page 18 for information on how to connect PTZ devices.

While the RS-485 connector can be used to connect a PTZ device, it is necessary that the device's protocol supports 'daisy chaining' in order to connect and control more than one camera (up to six).

Chaining the units allows them to share a single serial port. The protocol then decides which unit to address and sends commands to it specifically. See *Pin assignments*, on page 39 for pin assignment information.

RS-485 Connector (AXIS Q7900) – Usually used for connecting Pan Tilt Zoom devices. See *Pin assignments*, on page 39 for pin assignment information.

Pin assignments

Pin assignments for the I/O Connector of the AXIS 291 1U Video Server Rack

Pin	Function	Description	
1	+12V out, 100mA		
2	GND		
3	Channel 1, Configurable I/O 1	Digital input - Connect to GND to activate, or leave floating (or unconnected) to deactivate. Digital output - Uses an open-drain NFET transistor with the source connected to GND. If used with an external relay, a diode must be connected in parallel with the load, for protection against voltage transients.	Min input = - 40V DC Max input = + 40V DC Max load = 100mA Max voltage = + 40V DC (to the transistor)
4	Channel 2, Configurable I/O 1		
5	Channel 3, Configurable I/O 1		
6	Channel 4, Configurable I/O 1		
7	Channel 5, Configurable I/O 1		
8	Channel 6, Configurable I/O 1		
9	Channel 1, Configurable I/O 2		
10	Channel 2, Configurable I/O 2		
11	Channel 1, RS485A (non-inverting) (Video input 1)	A half-duplex RS-485 interface for controlling auxiliary equipment e.g. PTZ devices.	
12	Channel 1, RS485B (non-inverting) (Video input 1)		

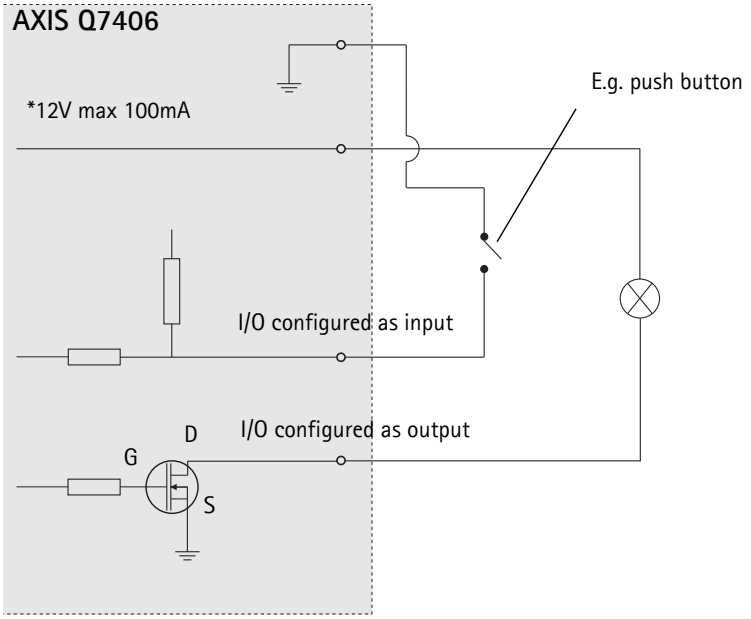
Note:

For I/O unit connector information for the AXIS Q7406 see page 40. For other video encoders, refer to their respective Installation Guide for I/O connector information.

Pin assignments for the I/O Connector of the AXIS Q7900 Rack

Pin	Function	Description	
1	Channel 1, Configurable I/O 1	Digital input - Connect to GND to activate, or leave floating (or unconnected) to deactivate. Digital output - Uses an open-drain NFET transistor with the source connected to GND. If used with an external relay, a diode must be connected in parallel with the load, for protection against voltage transients.	Min input = - 40V DC Max input = + 40V DC Max load = 100mA Max voltage = + 40V DC (to the transistor)
2	Channel 2, Configurable I/O 1		
3	Channel 3, Configurable I/O 1		
4	Channel 4, Configurable I/O 1		
5	Channel 5, Configurable I/O 1		
6	Channel 6, Configurable I/O 1		
7	Channel 1, Configurable I/O 2		
8	Channel 2, Configurable I/O 2		
9	Channel 3, Configurable I/O 2		
10	Channel 4, Configurable I/O 2		
11	Channel 5, Configurable I/O 2		
12	Channel 6, Configurable I/O 2		

The following connection diagram gives an example of how to connect an auxiliary device to the AXIS Q7406.



Pin assignments for the RS-485 Connector of the AXIS Q7900 Rack

Pin	AXIS Q7406
1	Channel 1, RS485A
2	Channel 1, RS485B
3	Channel 2, RS485A
4	Channel 2, RS485B
5	Channel 3, RS485A
6	Channel 3, RS485B
7	Channel 4, RS485A
8	Channel 4, RS485B
9	Channel 5, RS485A
10	Channel 5, RS485B
11	Channel 6, RS485A
12	Channel 6, RS485B

Note:

For RS-485 unit connector information for the AXIS Q7406 see *Unit connectors*, on page 38. For other video encoders, refer to their respective Installation Guide for I/O connector information.

Troubleshooting

Checking the Firmware

Firmware is software that determines the functionality of the video encoders. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem. The current firmware version in your encoder can be seen on the page **Setup > Basic Setup** or under **About.**

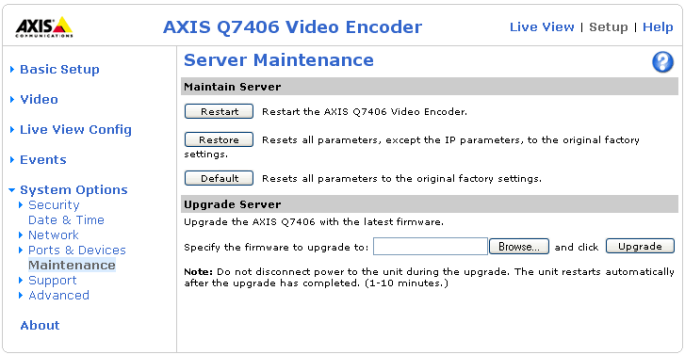
Upgrading the Firmware

When you upgrade your encoder with the latest firmware from the Axis Web site, your encoder receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release, before updating the firmware.

Note:

Preconfigured and customized settings are saved when the firmware is upgraded (providing the features are available in the new firmware) although this is not guaranteed by Axis Communications. Always read the instructions and release notes available with each new release, before upgrading the firmware.

1. Save the firmware file to your computer. The latest version of the firmware is available free of charge from the Axis website at **www.axis.com/techsup**
2. Go to **Setup > System Options > Maintenance** in the encoder's web pages.
3. In the **Upgrade Server** section, browse to the desired firmware file on your computer. Click **Upgrade**.



Notes:

- After starting the upgrade process, always wait at least 5-10 minutes before restarting the encoder, even if you suspect the upgrade has failed.
- Your dealer reserves the right to charge for any repair attributable to faulty upgrading by the user.
- The AXIS Camera Management software tool can be used for multiple upgrades. Please see the Axis website at www.axis.com for more information.

Emergency Recovery Procedure

If power or the network connection to the encoder is lost during the upgrade, the process fails and the unit becomes unresponsive. A flashing red Status LED indicates a failed upgrade. To recover the unit, follow the steps below. The serial number is found on the label attached to the bottom of the encoder.

1. **UNIX/Linux** - From the command line, type the following:
   arp -s <IP address of encoder> <serial number> temp
   ping -s 408 <IP address of encoder>

   Windows - From a command/DOS prompt, type the following:
   arp -s <IP address of encoder> <serial number>
   ping -l 408 -t <IP address of encoder>
2. If the unit does not reply within a few seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the encoder's IP address. In the page that appears, use the **Browse** button to select the upgrade file to use, for example, axisq7406.bin. Then click the Load button to restart the upgrade process.
4. After the upgrade is complete (1-10 minutes), the unit automatically restarts and shows a steady green on the Power and Status LEDs and flashing green or amber on the Network LED.
5. Reinstall the encoder, referring to the installation guide.

If the emergency recovery procedure does not get the encoder up and running again, please contact Axis support at www.axis.com/techsup/

Axis Support

If you contact Axis support, please help us to help you solve your problems by providing the server report, the log file and a detailed description of the problem.

Server Report - go to **Setup > System Options > Support > Support Overview**. The server report contains important information about the server and its software, as well as a list of the current parameters.

The **Log file** is available from **Setup > System Options > Support > Logs & Reports**. The Log file records events in the unit since the last system restart and can be a useful diagnostic tool when troubleshooting.

Symptoms, Possible Causes, and Remedial Action

Problems setting the IP address	
When using ARP/Ping	Try the installation again. The IP address must be set within two minutes after power has been applied to the encoder. Ensure the Ping length is set to 408. See the Installation Guide.
The encoder is located on a different subnet	If the IP address intended for the encoder and the IP address of your computer are located on different subnets, you will not be able to set the IP address. Contact your network administrator to obtain an appropriate IP address.
The IP address is being used by another device	Disconnect the encoder from the network. Run the Ping command. (In a Command/DOS window, type **ping** and the **IP address** of the unit). If you receive: **Reply from <IP address>: bytes = 32; time = 10 ms.....** - this means that the IP address may already be in use by another device on your network. You must obtain a new IP address and reinstall the unit. If you see: **Request timed out** - this means that the IP address is available for use with your encoder. In this case, check all cabling and reinstall the unit.
Possible IP address conflict with another device on the same subnet	The static IP address in the encoder is used before the DHCP server sets a a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the encoder. To avoid this, set the static IP address to 0.0.0.0.
The encoder cannot be accessed from a browser	
Problems with ONVIF	If ONVIF is not working as expected, it may be that for security reasons ONVIF was disabled when the camera was accessed over VAPIX. To enable ONVIF, reset the product to Factory default settings (see page 37).
The IP address has been changed by DHCP	If the encoder and client are on the same network, Run AXIS IP Utility to locate the encoder. Identify the encoder using its model or serial number Alternatively: 1) Move the encoder to an isolated network or to one with no DHCP or BOOTP server. Set the IP address again, using the AXIS IP Utility (see the Installation Guide) or the ARP/Ping commands. 2) Access the unit and disable DHCP in the TCP/IP settings. Return the unit to the main network. The unit now has a fixed IP address that will not change. 3) As an alternative to 2), if dynamic IP address via DHCP or BOOTP is required, select the required service and then configure IP address change notification from the network settings. Return the unit to the main network. The unit now has a dynamic IP address, but will notify you if the address changes.
Other networking problems	Test the network cable by connecting it to another network device, then Ping that device from your workstation. See instructions above.
Encoder is accessible locally, but not externally	
Broadband router configuration	To configure your broadband router to allow incoming data traffic to the encoder, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the encoder. This is enabled from **Setup > System Options > Network > TCP/IP Advanced**.
Firewall protection	Check the Internet firewall with your system administrator.
Default routers required	Check if you need to configure the default router settings.
Problems with the H.264 format	
No H.264 displayed in the client	Check that the correct network interface is selected in the AMC control panel applet (network tab).
	Check that the relevant H.264 connection methods are enabled in the AMC control panel applet (network tab).
	In the AMC control applet, select the H.264 tab and click the button Set to default H.264 decoder.
No multicast H.264 displayed in the client	Check with your network administrator that the multicast addresses used by the encoder are valid for your network.
	Check with your network administrator to see if there is a firewall preventing viewing.
Multicast H.264 only accessible by local clients	Check if your router supports multicasting, or if the router settings between the client and the server need to be configured. The TTL (Time To Live) value may need to be increased.
Poor rendering of H.264 images	Color depth set incorrectly on clients. Set to 16-bit or 32-bit color.
	If text overlays are blurred, or if there are other rendering problems, you may need to enable Advanced Video Rendering from the H.264 tab in the AMC control panel applet.
	Ensure that your graphics card is using the latest device driver. The latest drivers can usually be downloaded from the manufacturer's web site.

Color saturation is different in H.264 and Motion JPEG	Modify the settings for your graphics adapter. Please see the adapter's documentation for more information.
Lower frame rate than expected	Reduce number of applications running on the client computer.
	Limit the number of simultaneous viewers.
	Check with the system administrator that there is enough bandwidth available. See also the online help.
	Check in the AMC control panel applet (H.264 tab) that video processing is not set to **Decode only I frames**.
	Lower the image resolution.
Why do I not get 30 frames per second?	See the section. *General performance considerations,* on page 47
Image degeneration	Decrease the GOV length, see the online help for more information.
The Power indicator is not constantly lit	
Faulty power supply	Check that you are using an AXIS PS-H power supply.
The Status and Network indicator LEDs are flashing red rapidly	
Hardware failure	Contact your Axis dealer.
The Status indicator LED is flashing red and the encoder is inaccessible	
A firmware upgrade has been interrupted or the firmware has otherwise been damaged	See the *Emergency Recovery Procedure* above.
No images displayed on web page	
Problem with AMC. (*Internet Explorer only*)	To enable the updating of video images in Microsoft Internet Explorer, set your browser to allow ActiveX controls. Also, make sure that AXIS Media Control (AMC) component is installed on your workstation.
Installation of additional ActiveX component restricted or prohibited	Configure your encoder to use a Java applet for updating the video images under **Live View Config > Layout > Default Viewer** for Internet Explorer. See the online help for more information.
Video/Image problems, general	
Image too dark or too light	Check the video image settings. See the online help on Video and Image Settings.
Missing images in uploads	This can occur when trying to use a larger image buffer than is actually available. Try lowering the frame rate or the upload period.
Slow image update	Configuring pre-buffers, motion detection, high-resolution images, or high frame rates, will affect the performance of the encoder.
Poor performance	Poor performance may be caused by heavy network traffic, multiple users accessing the unit, low performance clients, use of features such as Motion Detection, Event handling, Image rotation other than 180 degrees.
Poor quality snapshot images	
Screen incorrectly configured on your workstation	In Display Properties, configure your screen to show at least 65000 colors, that is, at least 16-bit. Using only 16 or 256 colors will produce dithering artifacts in the image.
Overlay/Privacy mask is not displayed	
Incorrect size or location of overlay or privacy mask.	The overlay or privacy mask may have been positioned incorrectly or wrong resolution may have been used while positioning. Refer to the online help for information on the limitations when using image overlays and privacy masks.
Browser freezes	
Mozilla/Firefox 1.4 (or later) can sometimes freeze on a slow computer	Lower the image resolution.
Problems uploading files	
Limited space	There is only limited space available for the upload of your own files. Try deleting existing files to free up space.
Motion Detection triggers unexpectedly	
Changes in luminance	Motion detection is based on changes in luminance in the image. This means that if there are sudden changes in the lighting, motion detection may be triggered mistakenly. Lower the sensitivity setting to avoid problems with luminance.

For further assistance, please contact your reseller or see the support pages on the Axis website at www.axis.com/techsup

Technical Specifications

Item	Specification
Video compression	• H.264 • Motion JPEG
Resolutions	• 176x120 to 720x576
Frame rate H.264	30/25 (NTSC/PAL) fps in all resolutions
Frame rate Motion JPEG	30/25 (NTSC/PAL) fps in all resolutions
Video streaming	• Multi-stream H.264 and Motion JPEG • Controllable frame rate and bandwidth • VBR/CBR H.264
Image settings	• Compression, color, brightness, contrast, saturation • Rotation: 90°, 180°, 270° • Aspect ratio correction • Mirroring of images • Text and image overlay • Privacy mask • Enhanced deinterlace filter
Pan/Tilt/Zoom	• Wide range of analog PTZ cameras supported (drivers available for download at www.axis.com) • 100 presets/camera, guard tour, PTZ control queue • Supports Windows compatible joysticks
Users	20 simultaneous viewers
Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, digest authentication, user access log
Supported protocols	• IPv4/v6, HTTP, HTTPS, QoS layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, etc. • SSL/TLS* • *This product includes software developed by the Open SSL Project for use in the Open SSL Tool kit (www.openssl.org)
Application Programming Interface	• Open API for software integration, including VAPIX® from Axis Communications* • AXIS Media Control SDK*, event trigger data in video stream • Quality of Service (QoS) layer 3, DiffServ Model • Embedded Linux operating system • Support for AXIS Video Hosting System (AVHS) with One-Click Camera connection • Open API for software integration, including the ONVIF specification available at www.onvif.org *Available at www.axis.com
Intelligent video	Video motion detection, active tampering alarm
Alarm triggers	Intelligent video, external inputs, video loss
Alarm events	• File upload via FTP, HTTP and email • Notification via email, HTTP and TCP • External output activation • Local storage
Video buffer	64 MB pre- and post-alarm
Video access from web browser	• Camera live view • Video recording to file (ASF) • Customizable HTML pages • Windows XP, 2000, 2003 server • DirectX 9c or higher • For other operating systems and browsers see www.axis.com/techsup
Casing	Metal casing. Standalone or wall mount
Processor and memory	• 6x ARTPEC-3, 6x 128 MB RAM, 6x 128 MB Flash • Battery backed-up real-time clock

Item	Specification
Power	12 V DC, max. 15.4 W
Connectors	• 6 analog composite video BNC input, NTSC/PAL auto-sensing • 1000BaseT Ethernet • Terminal block for up to 12 configurable external inputs/outputs and up to 6 RS-485 half duplex, depending on the rack • Connectors, terminal block
Operating conditions	• 0-45 °C (32-113 °F) • Humidity 20-80% RH (non-condensing)
Approvals	• EN 55022 Class B, EN 61000-3-2, EN 61000-3-3, EN 55024, • EN 61000-6-1, EN 61000-6-2, FCC Part 15 Subpart B Class B, • ICES-003 Class B, VCCI Class B, C-tick AS/NZS CISPR 22, • EN 60950-1
Dimensions (HxWxD)	30 x 130 x 255 mm (1.2" x 5.1" x 10.0") excluding connectors
Weight	270 g (0.6 lb.)
Included accessories	• Installation Guide • CD with installation and management tools, software and User's Manual, 6 Windows decoder user licenses
Video management software (not incl.)	• AXIS Camera Station - Video management software for viewing, recording and archiving up to 25 cameras See www.axis.com/partner/adp_partners.htm for more software applications via partners

General performance considerations

When setting up your system, it is important to consider how various settings and situations will affect performance. Some factors affect the amount of bandwidth (the bit rate) required, others can affect the frame rate, and some will affect both. If the load on the CPU reaches its maximum, this will also affect the frame rate.

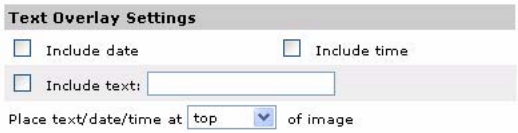
The following factors are among the most important to consider:

- High image resolutions and/or lower compression levels result in larger images. Bandwidth affected.
- Access by large numbers of Motion JPEG and/or unicast H.264 clients. Bandwidth affected.
- Simultaneous viewing of different streams (resolution, compression, etc.) by different clients. Bandwidth affected.
- Heavy usage of event settings affects the CPU load. Frame rate affected.
- Heavy network utilization due to poor infrastructure. Bandwidth affected
- Viewing on poorly performing client PC lowers perceived performance. Frame rate affected.

Optimizing your system

To see the bandwidth and frame rate currently required by the video stream, the video encoder provides a tool that can be used to display these values directly in the video image.

To do this, special format strings are added as part of a text overlay. Simply add **#r** (average frame rate in fps) and/or **#b** (average bandwidth in Kbps) to the overlay.



For detailed instructions, please see the online help for **Video & Image > Text Overlay Settings**, and the help for **File Naming & Date/Time Formats**.

Important!

- The figures displayed here are the values as delivered by the server. If other restrictions are currently in force, (e.g. bandwidth limitation) these values might not correspond to those actually received by the client.
- For Motion JPEG, these values will only be accurate as long as no frame rate limit has been specified.

Glossary

Active Speaker – a speaker with a built-in power amplifier.

ActiveX – A control (or set of rules) used by a browser. ActiveX controls are often downloaded and installed automatically as required.

AMC – AXIS Media Control. The control required for viewing video images in Internet Explorer. Installs automatically on first use.

API – Application Programming Interface. The Axis API can be used for integrating Axis products into other applications.

ARP – Address Resolution Protocol. Used to associate an IP address to a hardware MAC address. A request is broadcast on the local network to find out what the MAC address is for the IP address.

ARTPEC – Axis Real Time Picture Encoder – used for image compression.

Aspect ratio – A ratio of width to height in images. A common aspect ratio used for television screens and computer monitors is 4:3. High-definition television (HDTV) uses an aspect ratio of 9:16.

BOOTP – A protocol that can automatically configure a network device (give it an IP address).

Bonjour – Also known as zero-configuration networking, Bonjour enables automatic discovery of computers, devices, and services on IP networks. Bonjour allows devices to automatically discover each other without the need to enter IP addresses or configure DNS servers. Bonjour is developed by Apple Computer Inc.

CGI – Common Gateway Interface. A set of rules (or a program) that allows a Web Server to communicate with other programs.

Client/Server – Describes the network relationship between two computer programs, in which one, the client, makes a service request from another – the server.

DC-Iris – This special type of iris is electrically controlled by the Axis camera, to automatically regulate the amount of light allowed to enter.

dB (Decibels) – A unit to measure sound level changes. A 3dB change is the smallest level change we can hear. A 3dB change is actually twice or half the audio power level. A gain of 0dB will leave the signal level unchanged.

De-interlacing – De-interlacing is the process taking a stream of interlaced frames and converting it to a stream of progressive frames.

DSL – Digital Subscriber Line. A means of transferring data via standard phone lines.

Ethernet – A widely used networking standard.

ETRAX – Axis' own microprocessor.

Firewall – A virtual barrier between a LAN (Local Area Network) and other networks, e.g. the Internet.

FTP - File Transfer Protocol. Used for the simple transfer of files to and from an FTP-server.

Full-duplex - Transmission of data, e.g. audio, in two directions simultaneously.

G.711 - G.711 is the international standard for encoding telephone audio on 64 kbps channel. It is a pulse code modulation (PCM) scheme operating at 8 kHz sample rate.

G.726 - Frequently used speech-compression algorithm in telecommunications due to its high perceived speech quality and low resource requirements.

H.264 - Also known as MPEG-4 Part 10. This is the new generation compression standard for digital video. H.264 offers higher video resolution than Motion JPEG or MPEG-4 at the same bit rate and bandwidth, or the same quality video at a lower bit rate.

Half-duplex- A half-duplex link communicates in one direction at a time only, much like a walkie-talkie. Two way communication is possible, but not simultaneously.

HTTP – Hypertext Transfer Protocol. The set of rules for exchanging files (text, images, sound, video, and other files) on the World Wide Web.

HTTP-S (HTTPS)– An extension to the HTTP protocol to support sending data securely over the World Wide Web.

Intranet – A private network limited to an organization or corporation. Usually closed to external traffic.

IP – Internet Protocol. See TCP/IP.

IP address – A unique number used by a computer on the network to allow it to be identified and found.

ISMA – Internet Streaming Media Alliance.

JPEG – A standard image format, used widely for photographs. Also known as JPG.

LAN – A local area network (LAN) is a group of computers and associated devices that typically share common resources within a limited geographical area.

Linux – A popular operating system that is "open source" and practically free of charge.

Lux – A standard unit for light measurement.

Mbit/s – Megabits per second. A unit for measuring speeds in networks. A LAN might run at 10 or 100 Mbit/s.

MPEG-4 – A video compression standard that makes good use of bandwidth, and which can provide DVD-quality video streams at less than 1 Mbit/s.

Multicast – A bandwidth-conserving technology that reduces bandwidth usage by simultaneously delivering a single stream of information to multiple network recipients.

PEM – Privacy Enhanced Mail. An early standard for securing electronic mail. The PEM-format is often used for representing an HTTPS certificate or certificate request.

Ping – A small utility used for sending data packets to network resources to check that they are working and that the network is intact.

Pre/post alarm image – The images from immediately before and after an alarm.

Protocol – A special set of rules governing how two entities will communicate. Protocols are found at many levels of communication, and there are hardware protocols and software protocols.

(QoS) Quality of Service – QoS provides the means to guarantee a certain level of a specified resource to selected traffic on a network. Quality can be defined as e.g. a maintained level of bandwidth, low latency, no packet losses, etc.

Router - A device that determines the next network point to which a packet should be forwarded on its way to its final destination. A router is often included as part of a network switch (see below).

RTP- Real-Time Transfer Protocol. A transfer protocol designed for the delivery of live content, e.g. MPEG-4.

RTSP (Real Time Streaming Protocol) - RTSP is a control protocol, and a starting point for negotiating transports such as RTP, multicast and Unicast, and for negotiating codecs. RTSP can be considered a "remote control" for controlling the media stream delivered by a media server. RTSP servers typically use RTP as the protocol for the actual transport of audio/video data.

Simplex - In simplex operation, a network cable or communications channel can only send information in one direction; it's a "one-way street".

SMTP - Simple Mail Transfer Protocol is the protocol used to send e-mail across the Internet. SMTP authentication is a way of allowing people outside of a domain to use an SMTP server when sending e-mail.

SNMP - Simple Network Management Protocol. An application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.

Subnet Mask - An IP address consists of two components: the network address and the host address. "Subnetting' enables a network administrator to further divide the host part of the address into two or more subnets. The subnet mask identifies the subnet to which an IP address belongs.

Switch - Whilst a simple hub transmits all data to all devices connected to it, a switch only transmits the data to the device it is specifically intended for.

TCP/IP - Transmission Control Protocol/Internet Protocol. A suite of network protocols that determine how data is transmitted. TCP/IP is used on many networks, including the Internet. TCP keeps track of the individual packets of information and IP contains the rules for how the packets are actually sent and received.

UDP - The User Datagram Protocol is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is also known as UDP/IP.

Unicast - Communication between a single sender and a single receiver over a network. A new connection is established for each new user.

URL - Uniform Resource Locator. An "address" on the network.

Varifocal - A varifocal lens provides a wide range of focal lengths, as opposed to a lens with a fixed focal length, which only provides one.

WAN - Wide-Area-Network. Similar to a LAN, but on a larger geographical scale.

Web server - A program on a computer that delivers the resources (usually web pages) requested by the web user (the client).

Index

A
Action 24
Action Buttons 9, 16
Active/Inactive 17
Administrator 12
Alarm 27
AMC 6
ARP/Ping 31
AVHS 31

B
Bit Rate 12
Bonjour 6
Buffer Size 25
Buffers 25

C
CGI links 22
Click-in-image 22

D
Date & Time 30
Default Viewer 15
DNS Configuration 33
DNS Server 33
Domain Name 33

E
Emergency Recovery 42
Enable ARP/Ping 31
Event Servers 24
Events 24

F
Frame Rate 12
FTP Server 24

G
GOV Settings 12

H
Host Name 33
HTTP API 22
HTTP Server 24
HTTP-API 11
HTTPS 7, 8, 29

I
I/O Ports 35
Installing PTZ devices 18
IP Address Filtering 29

L
Live View Config 15
Logs & Reports 36

M
Motion Detection 27

N
NAT traversal 7, 33
Network Settings 31
NTP Server 30

O
Output Buttons 17

P
Pan/Tilt/Zoom 21
Port Status 28
Ports & Devices 35
Post-trigger Buffer 25
Preset positions 19
Pre-trigger Buffer 25
PTZ commands 22
PTZ control queue 20
Pulse 17

Q
QuickTime 11, 15

R
Recovery 42
Referrals 29
Relative and absolute PTZ drivers 22
Restore 36

S
Scheduled Event 24, 26
Security 29
Server Time 30
SNMP 35
Specifications 46

Support 36
System Options 29

T
TCP Server 24
TCP/IP Settings 31
Time Mode 30
Triggered Event 24
Troubleshooting 42

U
Upgrade Server 36
UPnP 33, 35
Users 29

V
Video Stream 12
Video streams 10